



Right to Privacy and Personal Autonomy in IoMT: Exploring the Principles of Privacy and Autonomy in the Contemporary Paradigm

Rebant Juyal^{1,*}  and Avnish Bhatt² 

¹ Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology, Kharagpur, India

² Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology, Kharagpur, India

rb.juyal27@gmail.com

Abstract. The Internet of Medical Things (IoMT) has brought a monumental change in the very essence of healthcare by offering path-breaking innovative solutions for medical diagnosis, treatment, and surveillance. However, safeguarding the personal autonomy of people associated within the wide spectrum of the Internet of Medical Things persists as the most intrinsic and sacrosanct objective and obligation of the service providers. Furthermore, the need to preserve personal autonomy in the context of IoMT involves the need to safeguard the right to individual privacy in the virtual world. This article tries to examine and explore the relevance and risks associated with the right to privacy and confidentiality in IoMT. It highlights the subjective aspect of the right to privacy and personal autonomy.

Keywords: Right to Privacy, Personal Autonomy, IoMT.

1 Introduction

Technology persists as an integral component of society today. With the accelerated developments and globalisation in the 21st century, every institution, including society's critical infrastructure, is virtually dependent upon technology usage. The increasing use of technology has consequently brought the issue of privacy into the limelight. While technological advancements remain imperative in society, it also remains indispensable to protect, preserve and safeguard the Right to Privacy of the individuals living in the society. The advent of the Internet of Things (IoT) has fundamentally revolutionised various aspects of an individual's life, and as a consequence, the healthcare sector stands no exception to these breakaway rearrangements. The Internet of Medical Things (IoMT) finds its relevance in this regard. IoMT refers to a "network of interconnected medical devices, wearables, sensors, and software applications which collect and exchange health data on a real-time basis" (Huang et al., 2023).

The emerging field of IoMT holds immense significance in terms of its unprecedented potential to improve healthcare outcomes. The modish technologically oriented specie of the contemporary Internet of things enables monitoring of patient remotely (Damera et al., 2025). The unique feature of remote monitoring further enables enhanced medical diagnostics and also facilitates in the personalised treatment approaches (Mathkor et al., 2024). The unprecedented advantages offered under IoMT regime has accelerated its integration within the existing healthcare system of our society. However, as the modern technological framework of IoMT continues to evolve, it stands crucial to consider and examine its potential implications over the subjective domain of individual privacy and personal autonomy (Ahmed et al., 2025). While, the norm of personal autonomy mandates that individuals must enjoy the liberty to make informed decisions concerning their own health by exercising agency in healthcare choices autonomously, privacy commands preservation of medical information from external inferences and individual's control over it. This article scrutinizes the quintessential imperatives of confidentiality and autonomy in the IoMT paradigm and the existential threats juxtaposed towards privacy of the person. The article undertakes a doctrinal analysis of the extant juridical and policy instruments parsing the constitutional provisions, statutory regulations and case laws. For scholarship precision the article analyses examples various legal scholarships

2 Right to Privacy

The Indian Constitution provides a diverse spectrum of rights with individual and collective rights being its part. It remains the duty of constitutional courts to maintain the harmony between the individual and group rights in cases of competing interests. Since, the constitution itself does not pose one right above the other; it is left to the interpretation of the text to harmonise the competing claims of group versus individual (Dwivedi et al., 2022), the incident of which occurs between the right to privacy and right to information. While construing the competing claims under group rights and individual rights, the court leans in favour of constitutional morality, which in turn derives from a liberal idea of society where individualism outlaws the conservative collective belief; however, this path of achieving the highest standard of aspiration for the individual is incidentally subjected to group rights as well (*Navej Singh Johar v. Union of India*, AIR 2018 SC(CRI) 1169; *Indian Young Lawyers Association v. State of Kerala*, (2018) 11 SCC 1; Gutwirth & Hert, 2021).

Recognising Right to Privacy as a right within the collective constitutional scheme of Article 14, 19 and 21 under Part III of the Indian Constitution, in the *Justice K.S. Puttaswamy vs. Union of India* case [(2017) 10 SCC 1], the court sanctioned a three-fold requirement for the invasion to the privacy right (Kumar, 2019). The three tests are as follows:

1. Legality- There ought to be some statutory enactment empowering the authority to make out the invasion of privacy.
2. Need- There must be a legitimate state's aim; the legitimacy of such an action arises from the fulfilment of public interest. This test persists imperative in balancing

the two counterclaims of privacy and public good. It provisions the overpowering of public benefit against individual privacy claims in cases of legitimate requirements.

3. Proportionality- The proportionality test determines if the information sought to be disclosed has any nexus with the public interest to be served, if the information sought to be disclosed doesn't serve any public interest, and confidentiality is important to be kept, then the authority can deny access to the information, which the authority keeps in a fiduciary capacity.

3 Notion of Constitution

The freedom of speech and expression ascribed under Article 19 put forward the aspiration of the constitution to have an informed citizenry. Article 19(1)(a) imposes on the government not just the negative obligation to prohibit itself from restricting the citizen's right to access to information, but simultaneously sanctions a positive obligation for public disclosure of information. The framers of the Indian constitution had in mind the notional concept of participatory form of democracy. To this spirit the Indian Supreme Court in *Rajeev Suri vs. Delhi Development Authority* (2021 SCC OnLine SC 8) noted, "A holistic understanding of the dispensation envisaged under our Constitution would reveal that we are a representative democracy with strong elements of participatory democracy embedded in it." Therefore, accessibility to information is *sine qua non* for participatory democracy. In the case of *S P Gupta v. Union of India* (AIR 1982 SC 149) it was observed by Justice PN Bhagwati:

"The citizens have a right to decide by whom and by what rules they shall be governed and they are entitled to call on those who govern on their behalf to account for their conduct. No democratic Government can survive without accountability and the basic postulate of accountability is that the people should have information about the functioning of the Government"

Whereas, information and access to information stands as one of the important of governances and also access to informative data including the medial data persists intrinsic for business operations, digital health governance (Van Den Hoven, 2008), among others, privacy also stands quintessential in its existence to protect, preserve and safeguard the personal liberty, autonomy and dignity of the individual. Furthermore, the concept of privacy is not restrictive rather spreads across various dimensions and kinds (Koops et al., 2017, p. 556). Deliberating on various dimensions of privacy the SC in *Puutaswamy* judgment noted:

"The nine primary types of privacy are, according to the above depiction: (i) bodily privacy which reflects the privacy of the physical body. Implicit in this is the negative freedom of being able to prevent others from violating one's body or from restraining the freedom of bodily movement; (ii) spatial privacy which is reflected in the privacy of a private space through which access of others can be restricted to the space; intimate relations and family life are an apt illustration of spatial privacy; (iii) communicational privacy which is reflected in enabling an individual to PART M restrict access to communications or control the use of information which is communicated to third parties; (iv) proprietary privacy which is reflected by the interest

of a person in utilising property as a means to shield facts, things or information from others; (v) intellectual privacy which is reflected as an individual interest in the privacy of thought and mind and the development of opinions and beliefs; (vi) decisional privacy reflected by an ability to make intimate decisions primarily consisting one's sexual or procreative nature and decisions in respect of intimate relations; (vii) associational privacy which is reflected in the ability of the individual to choose who she wishes to interact with; (viii) behavioural privacy which recognises the privacy interests of a person even while conducting publicly visible activities. Behavioural privacy postulates that even when access is granted to others, the individual is entitled to control the extent of access and preserve to herself a measure of freedom from unwanted intrusion; and (ix) informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information."

To emphasise the constitutionally imperative relevance of privacy after analysing the diverse species of privacy, the court in its judgement further noted-

"Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III. Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture."

The above reading of the Indian Supreme Court judgment sanctions the inclusion of the Right to privacy within the Indian constitutional scheme.

4 Tussle Between the Competing Rights

The right to privacy is a constitutionally protected right under Article 21 from the text of 'right to life and personal liberty' which guarantees freedom and dignity. Dignity of an individual is a facet of his or her right of privacy; however, it is to be noted that the preamble of our constitution put forward the objective of assuring dignity to the individual (Kumar, 2019). This constitutional objective is sought through Article 21. Recognising the right of privacy and stretching it to several aspects of an individual's societal identity ultimately strengthens the object of assurance of the dignity of an individual. The restriction on the right to privacy needs to be imposed carefully, as it also threatens the dignity of an individual, which is why it needs to be provided by law, in a legitimate state's aim and needs to be proportional. The proportionality to the restriction is in regard to the extent of abridgement of the right with a legitimate state's aim. The right to privacy not only encompasses personal intimacies but also extends to decisional and informational autonomy. An individual has a right over his or her personal information and its dissemination; therefore, an unwarranted abridgement will amount to a violation of a fundamental right.

5 Personal Information

The proposition of protection of privacy against technology, is to be seen in the context of protecting personal information in digital space including the collection and use of medical information by private and government entity under the umbrella of digital health governance mechanism and also aspect of the control of individuals over their data after they have submitted to avail the benefits of services (McGraw & Mandl, 2021).

Section 2(i) of the Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011 defines the term —personal information‖ in the following terms: — ‘Personal information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person’.

Article 4(1) of the EU General Data Protection Regulation (GDPR) defines personal data in similar terms: —Personal data‘ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.

The protection of personal information was recognised by the courts in South Africa as a facet of the right to privacy in the case of *National Media Ltd v. Jooste* [1996 (3) SA 262 (SCA)] where the court observed

“A right to privacy encompasses the competence to determine the destiny of private facts. The individual concerned is entitled to dictate the ambit of disclosure e g to a circle of friends, a professional adviser or the public. He may prescribe the purpose and method the disclosure. Similarly, I am of the view that a person is entitled to decide when and under what conditions private facts may be made public.”

The protection of personal information arises from the fact that the dissemination of such information may impact the dignity of such an individual (Graham, 1987). Although under the Indian constitutional scheme, even if the dissemination does not impact upon the dignity or image in the public sphere of an individual, the information sought can still be denied if it does not serve any ‘larger public interest’. Therefore, the balancing sides under this interplay of rights are concerned with the confidentiality of the information, which is considered as ‘personal’ and ‘public interest’.

6 The Role of Privacy in Preserving Personal Autonomy

6.1 Connection between privacy and personal autonomy in IoMT

The subject of privacy and personal autonomy draws a central role in the subjective domain of the Internet of Medical Things. Personal liberty in reference to various legal

scholarships can be understood in simple words as the ability of the individual to exercise its own control over its own body. Personal autonomy mandates that individuals make their own informed decisions concerning the subject of their health and further determine the course of their medical treatment with absolute autonomy and freedom and without any undue influence. It is on account of the notional postulation of the Privacy right that individuals enjoy the freedom to preserve the confidentiality of their intimate health related data and make subsequent choices autonomously that is in absence of any external interference. To this abstraction, it emerges pertinent to state that to the sacrosanct conception of personal autonomy, privacy acts as its foundational element. It empowers individuals preserve a sense of personal agency in their respective healthcare decisions. Moreover, its ordained legal framework gives confidence to the patients to seek medical advice, assess and also explore different treatment options, and further disclose deeply personal and sensitive health-related medical information with healthcare personnel without the fear of judgments or any form of unwarranted disclosures through any unauthorised means. Safeguarding the dimension of intimate health data, privacy upholds human dignity the informational self-determination of the person. Protection of these sacrosanct fundamentals thereby, reinforces the notion of individual personal autonomy which enables people to undertake their respective healthcare decisions in accordance to their preferences and individual circumstances including the practical realities of the situation. Additionally, the robust privacy protection fosters the trust towards the digital healthcare systems which emerges intrinsic to enable effective patient engagement and informed-decision making.

6.2 Ensuring informed consent and control over personal health data

The fundamental norm of personal autonomy of the individual within the IoMT regime mandates sanctioning of an effective framework wherein the individual person is guaranteed to be given an informed consent and the person further ensues control over his or her intimate and personal data. The notion of informed consent provisions that the patient must be provided with clear and easily understandable information concerning the collection of health-related data by the IoMT devices and the applications within the network and its further usability that is how the data will be used, stored and shared in future. Institutionalisation of the informed consent norm shall enable people to make voluntary and a more aware decisions concerning their personal health data.

Moreover, the contemporary IoMT framework must empower people to exercise absolute control over their health data. Provisioning of absolute control would give people with diverse inherent rights, like the right to access, modify, and also the authority to obliterate their intimate data from the network, and the right to restrict its applicability, mandating who can use it and that too for the prescribed purpose only. This would enable people to enjoy true ownership and agency over their medical information and reinforce the fundamentals of personal autonomy in the contemporary digital healthcare network.

6.3 Maintaining confidentiality and trust in healthcare relationships

Confidentiality and trust are basic components of any healthcare relationship. Furthermore, privacy in the Internet of Medical Things (IoMT) is critical in ensuring confidentiality and trust between individuals and healthcare providers (Ahmed et al., 2025). If individuals are confident that their private health informatics information will be handled with confidentiality, they will be encouraged to access healthcare services and provide information, which will help in creating a free and comfortable environment for communication with healthcare providers. IoMT can create a platform that will provide individuals with the freedom to share their private health information electronically while respecting privacy.

Furthermore, healthcare providers, in turn, can utilise this information to deliver tailored and effective care, resultantly promoting personal autonomy in the decision-making process. Ensuring the confidentiality of health-related data also safeguards people from potential stigmatisation or even any form of discrimination, which could be based on their medical history, empowering them to exercise autonomy without fear of repercussions.

7 Threats to Privacy Rights in the Digital Age

7.1 Data breaches and unauthorised access to personal health information

There emerges an urgent need to balance the usage of technology, surveillance and fundamental right to privacy of the people. The contemporary data-oriented model wherein even the intimate health data can be possibly retained convincingly appears antithetical to the human right of Privacy. While, as per Indian Constitution fundamental rights are not enforceable against the private corporations but, the fundamental notion of human rights postulates that they are respected, preserved and protected by every entity including Private Corporations. Therefore, the private sector undertakings must align their policies with the spirit of Right to Privacy. Continuous instances of data breaches and unauthorised access to private health information emerge as one of the foremost threats to privacy rights in the contemporary digital age (Seh et al., 2020). With the expansion of the IoMT landscape, the volume of sensitive health data being collected, stored and transmitted also proliferates (Alsaeed & Nadeem, 2025). This vast amount of personal information resultantly becomes an attractive target for malicious actors seeking to exploit vulnerabilities in the existing security systems. Data breaches, therefore, can amount to unauthorised access to any person's personal or private medical records, exposing highly intimate and sensitive information to the public or even to criminals or anti-social elements. Such breaches violate privacy rights and have far-reaching implications, which also include threats like identity theft, fraud, and reputational damage.

7.2 Potential misuse of health data for commercial purposes

The potential misuse of health data for commercial purposes persists as another concerning threat to privacy rights in the contemporary digital age (Paul et al., 2023). With the mushrooming development of IoMT devices and applications, extensive amounts of health information are being collected, at times even without the individual's full awareness and understanding. This enormous wealth of data holds invaluable significance for diverse and difference stakeholders including different pharmaceutical companies, insurance providers, and others. Consequently, the potential possibility of exploiting valuable personal health data of individuals could be exploited for targeted advertisement, profiling of individuals based on their medial history or other medical information cannot be denied. These critical possibilities therefore, provisions convincing ground of concern regarding the enormous possibility of compromising with the privacy and personal liberty of the individual. Occurrence of such instances can further lead to discriminatory practices with individual people based on their health data. Additionally, the commodification of the health-related data further give rise to ethical concerns since, the divergently competing idea of health data commodification challenges and stands antithetical to the very fundamental principal of ethics in this field that personal health information must be solely used for improving the individual healthcare outcomes and must not be exploited for other uses.

7.3 Surveillance concerns and implications for personal autonomy

As discussed, privacy and personal autonomy of the individual are integral to their existence (Henkin, 1974; Levi, 1978). However, the unprecedented proliferation of surveillance technologies in various avenues and dimensions and their further integration into the IoMT systems raises serious concerns with regard to the subject of privacy and the personal autonomy of individuals (Jawad,2024). Even though, with the aid and assistance of the advanced surveillance technologies, the possibility of potentially improving the healthcare monitoring and also the early detection of medical conditions increases (Abdulmalek et al., 2022; Singhal et al., 2025). However, the pervasive nature of the surveillance technologies especially with respect to the domain of IoMt can fundamentally transgress the constitutionally safeguarded sacrosanct spectrum of individual privacy of the people. Therefore, continuous monitoring and tracking of intimate personal health information of a person, particularly in cases when conducted without the informed consent and explicit knowledge of the designated person, can lead to the creation of a surveillance society wherein autonomy stands destined to be eroded by technologically driven pervasive framework. Moreover, the Indian Supreme Court has recognised the Right to Privacy as fundamental right under Article 21 that is Part III of the Indian Constitution. The recognition of privacy as a fundamental right, grants it with one additional characteristic of inviolability that is just like other fundamental rights, individual consent can never be considered as a basis for relinquishment of the fundamental right to privacy. Therefore, it becomes indispensable that beyond the scope of individual consent the state must take necessary steps including at the legislative front, that within the framework of IoMT, the intimate personal date of the people

is not merely collected merely on the basis of individual consent rather, the data collection exercise must also satisfy the previously discussed norms of Necessity, Fairness and Proportionality.

The constant presence of monitoring devices can also lead to self-censorship or even the alteration of behaviour, thereby limiting the ability of each individual to make an independent choice about their health. Therefore, a surveillance-driven environment can potentially undermine personal autonomy by exerting external influence and control over the actions and decisions of every person.

8 Conclusion: Safeguarding Privacy Rights in IoMT

8.1 Legislative and regulatory measures to protect privacy in the digital age

In order to preserve and protect privacy rights in the IoMT landscape, robust legislative and regulatory measures must be adopted. The State must play a crucial role in enacting effective frameworks to safeguard individual privacy rights in the contemporary digital age. The imperative constitutional scheme provisioned within the harmonious and conjoint reading of Article 14, 19 and 21 of the Indian Constitution mandates a constitutional prescription over to the state to preserve, protect and safeguard the privacy of the people. In furtherance of this constitutional prescription, the state must enact specific and targeted legislative enactments focusing on the domain of Interment of Medical things. While, the Data protection law has been enacted very recently, however the state can also consider instituting few advanced statutory and executive steps to address the unique challenges the IoMT landscape poses. The regulations must clearly outline specific guidelines over crucial subjects like data collection, storage, access, and sharing of health-related medical data of the people. This shall ensure that the personal health information of each person is handled with utmost care which would provide an effective impetus for the flourishing of the digital health governance framework in India, in accordance with the mandate of the sacrosanct fundamental right to privacy guaranteed under Article 21 of the Indian Constitution. Furthermore, regulatory bodies could also enforce strict penalties in cases of non-compliance since it would serve as a deterrent for entities that may seek to disregard the right to privacy and other considerations associated with it.

8.2 Promoting privacy-enhancing technologies and encryption

Preserving the autonomy and privacy of the individual stands as an indispensable imperative to value the spirit of human rights (Kupfer, 1987). In this regard, there emerges a mandatory requirement to promote the adoption, applicability and usages of such advanced technologies which enhances the framework of safeguarding privacy. Further, to preserve the privacy rights of the individual in the regime of Internet of Medical things, encryption of data and applying the encryption technology at all required forums and levels in this realm stands necessitated with paramount considerations. Adoptions

of the encryption technology stands imperative since, such technique would effectively ensure that private health information remains securely transmitted and stored, thereby reducing the risk of unauthorised access and even data breaches. Privacy-enhancing technologies, like differential privacy and de-identification methods, can also anonymise data and simultaneously allow for meaningful analysis and research. By encouraging the adoption of such technologies, healthcare organisations and technology providers can strengthen the privacy safeguards and, consequently, instil confidence among individuals that their data remains protected.

8.3 Educating individuals about their privacy rights and encouraging active participation in decision-making

Empowering individuals with knowledge about their respective privacy rights and actively involving and engaging them in the decision-making process stands vital to safeguard privacy in the IoMT arena. Further, educational initiatives must also be implemented to increase awareness about privacy concerns in the digital healthcare realm. Since by fostering an informed and engaged population, people can make choices that may align with their respective privacy preferences, enable them to participate in discussions surrounding privacy policies actively, and further hold stakeholders accountable for upholding the privacy rights of the people.

Acknowledgments. The author had no funding for this article.

Disclosure of Interests. The author has no Competing Interests.

Generative AI Use Disclosure: Not Applicable

References

1. Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaia, M. A. M., Bairagi, A. K., Khan, Md. A.-M., & Kee, S.-H. (2022). Iot-based healthcare-monitoring system towards improving quality of life: A review. *Healthcare*, 10(10), 1993. <https://doi.org/10.3390/healthcare10101993>
2. Ahmed, S. F., Sharmin, S., Kuldeep, S. A., Lameesa, A., Alam, Md. S. B., Liu, G., & Gandomi, A. H. (2025). Transformative impacts of the internet of medical things on modern healthcare. *Results in Engineering*, 25, 103787. <https://doi.org/10.1016/j.rineng.2024.103787>
3. Alsaeed, N., & Nadeem, F. (2025). AI-enabled IoMT: Transforming healthcare in smart hospitals. In *Blockchain and Digital Twin for Smart Hospitals* (pp. 459–496). Elsevier. <https://doi.org/10.1016/B978-0-443-34226-4.00024-1>
4. Damera, V. K., Cheripelli, R., Putta, N., Sirisha, G., & Kalavala, D. (2025). Enhancing remote patient monitoring with AI-driven IoMT and cloud computing technologies. *Scientific Reports*, 15(1), 24088. <https://doi.org/10.1038/s41598-025-09727-z>
5. Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of Internet of Medical Things (Iomt) applications in building a smart healthcare system: A systematic review. *Journal of*

- Oral Biology and Craniofacial Research*, 12(2), 302–318. <https://doi.org/10.1016/j.jobcr.2021.11.010>
6. Graham, J. P. (1987). Privacy, computers, and the commercial dissemination of personal information. *Texas Law Review*, 65(7), 1395–1440.
 7. Gutwirth, S., & Hert, P. (2021). Human rights: A secular religion with legal crowbars. From europe with hesitations. *National Law School of India Review*, 33(2). <https://repository.nls.ac.in/nlsir/vol33/iss2/9>
 8. Henkin, Louis. (1974). Privacy and autonomy. *Columbia Law Review*, 74(8), 1410–1433.
 9. Huang, C., Wang, J., Wang, S., & Zhang, Y. (2023). Internet of medical things: A systematic review. *Neurocomputing*, 557, 126719. <https://doi.org/10.1016/j.neucom.2023.126719>
 10. Jawad, L. A. (2024). Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. *Abhigyan*, 42(1), 23–31. <https://doi.org/10.1177/09702385241233073>
 11. Koops, B.-J., Newell, B., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, 38(2), 483. <https://scholarship.law.upenn.edu/jil/vol38/iss2/4>
 12. Kumar, V. (2019). Dynamics of The ‘Right to Privacy’: Its Characterization Under The Indian Constitution. *Journal of Indian Law Institute*, 61(1). <https://doi.org/https://www.jstor.org/stable/27097351>
 13. Kupfer, J. (1987). Privacy, Autonomy, and Self-Concept. *American Philosophical Quarterly*, 24(1), 81–89. <http://www.jstor.org/stable/20014176>
 14. Levi, D. R., & Sporleder, T. L. (1978). Some recent interpretations of the capper volstead act: legal economic analysis. *Idaho Law Review*, 14(2), 435–446.
 15. Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (Iomt) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. *Journal of Infection and Public Health*, 17(4), 559–572. <https://doi.org/10.1016/j.jiph.2024.01.013>
 16. McGraw, D., & Mandl, K. D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *Npj Digital Medicine*, 4(1), 2. <https://doi.org/10.1038/s41746-020-00362-8>
 17. Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 9(4), 571–588. <https://doi.org/10.1016/j.icte.2023.02.007>
 18. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, 8(2), 133. <https://doi.org/10.3390/healthcare8020133>
 19. Singhal, V., R., S., Singhal, S., Tiwari, A., & Mangal, D. (2025). Healthcare and cutting-edge technology: Advancements, challenges, and future prospects. *Computers in Biology and Medicine*, 196, 110861. <https://doi.org/10.1016/j.compbimed.2025.110861>
 20. Van Den Hoven, J. (2008). Information Technology, Privacy, and the Protection of Personal Data. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 301–321). chapter, Cambridge: Cambridge University Press.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

