https://doi.org/10.37420/j.mlr.2025.005

The Data Governance in Public Health Emergencies

Zheng Huo[1] ,Huimiao Zhao[2*]
[1]Assistant Researcher, Institute of Law and Intellectual Property, Beijing University of Chemical Technology, Beijing, China.
[2]Executive Director, the Institute of Law and Intellectual Property, Beijing University of Chemical Technology, Beijing, China.
[*]Corresponding author, E-mail:zhaohuimiao@mail.buct.edu.cn

Abstract
In recent years, the frequent occurrence of global public health crises has brought data governance to the forefront of legal and policy discussions. This paper examines how to reconcile the imperative of data openness and information sharing with the need to safeguard personal sensitive information in the context of public health emergencies. By analyzing the pivotal role of big data in such crises, it underscores its significance in epidemic prediction, real-time monitoring, policy decision-making, and the allocation of healthcare resources. After delineating the legal connotations of data rights, the paper explores the statutory and ethical frameworks governing data accessibility and protection. Ultimately, it emphasizes the necessity of ensuring the security of personal information while advancing the public interest, thereby seeking to strike a legally sound and ethically balanced approach to data governance.

Keywords
Public Health Emergencies; Data Governance; Data Openness; Information Protection

1 Introduction

With the rise of digital governance, big data technology has become integral to the effective management of public health emergencies. This process entails the handling of vast amounts of personal information, government data, and epidemic-related datasets. A critical question arises: how should these data be lawfully processed? In the collection and sharing of such information, how can individuals' privacy rights be adequately protected? Moreover, how should data be appropriately disclosed while ensuring robust safeguards during public health crises? These pressing legal and ethical concerns merit thorough examination.

2 Forms of Data Rights Involved in Public Health Emergencies

Public health emergencies often involve vast amounts of personal information, public data, and cross-border data flows. These data not only pertain to individual privacy and autonomy but also have significant implications for public safety and national interests [1]. In critical processes such as risk prevention and control, as well as the allocation of medical resources, the collection, analysis, and sharing of personal health data play an essential role [2]. However, improper handling or misuse of such data can infringe upon individual privacy

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

rights, creating tensions between personal data protection and the broader public interest. Consequently, in the context of public health emergencies, the delineation of data rights must consider the complex interplay of individual, collective, and state interests while maintaining a delicate balance among legal, ethical, and practical considerations.

Effectively managing public health emergencies requires collaboration among multiple stakeholders, including individuals, government agencies, private enterprises, and social organizations. The involvement of these diverse entities leads to an expansion of data types within public health incidents. This paper posits that, under such circumstances, the primary categories of data involved are personal data and public data.

Personal data refers to information derived from individual identities and activities. In public health crises, it can generally be classified into three categories: identity data, medical data, and itinerary data. Identity data includes personally identifiable information (PII) such as names, national identification numbers, and residential addresses. Medical data encompasses an individual's medical history, diagnostic records, and treatment information. Itinerary data pertains to an individual's significant travel movements and locations visited. Based on its sensitivity, personal data can be further categorized as general personal data or sensitive personal data [3]. The distinction lies in whether unauthorized disclosure, misuse, or abuse of the data could compromise personal or financial security, damage reputation, cause psychological or physical harm, or result in discriminatory treatment. During public health emergencies, heightened societal anxiety often amplifies scrutiny of confirmed or suspected patients. Under such conditions, even general personal data may be extensively mined by the media and the public, effectively elevating it to the status of sensitive data [4]. Consequently, ensuring the protection of personal data and precisely defining sensitive personal data within the framework of a public health emergency is of paramount importance.

The definition of public data remains a topic of debate in legal and academic discourse [5]. Opinions of the CPC Central Committee and the State Council on Establishing a Fundamental Data System to Better Leverage the Role of Data as a Factor of Production defines public data as information generated by government bodies and enterprises in the course of performing official duties or providing public services [6]. In the context of a public health emergency, public data can be categorized into two primary types. The first consists of data collected and generated by various government agencies—including health authorities, disease control institutions, market regulators, transportation departments, and public security organs—in executing their statutory responsibilities related to risk monitoring, epidemic prevention and control, medical treatment, resource allocation, traffic management, and public security. The second category comprises data contributed by public institutions such as hospitals, research organizations, and grassroots community service providers in the context of epidemic prevention and response. Collectively, these data sources constitute epidemic-related public data.

In managing public health emergencies, a government-led, enterprise-participatory cooperative model has become an established practice. Although a substantial portion of data is gathered through collaborative efforts between government authorities and private entities or institutions, the government remains the ultimate data controller and bears primary responsibility for data collection, storage, processing, transmission, and disclosure [7]. Enterprises and institutions involved in such collaborations are legally bound by

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

confidentiality and data security obligations as stipulated in their agreements with the government [8]. Accordingly, in public health emergencies, whether data is acquired directly by governmental agencies in the execution of their statutory duties or generated through government-led cooperation with private enterprises or institutions, it qualifies as public data.

3 Data Openness in Public Health Emergencies

3.1 Basis for Data Openness

The right to personal information is a fundamental constitutional right, encompassing both the right to informational self-determination and the right to personal information protection. The state assumes a dual obligation: a negative duty to refrain from excessive collection and misuse of personal information, and a positive duty to safeguard individuals from discriminatory or unfair treatment by data processors [9]. In the context of public health emergencies, data transparency enables the government and relevant authorities to swiftly and accurately assess the situation, thereby enhancing the protection of public interests. Given that public health crises often involve the rapid transmission of infectious diseases that pose severe threats to public health and life, the protection of the rights to life, health, and public safety takes precedence over the right to personal information [10]. Furthermore, in risk prevention and crisis management, the principle of necessity permits limited derogations from personal data protection norms, subordinating individual interests to the overriding public interest—an approach widely recognized in international legal practice. The urgent and public nature of health emergencies necessitates a reasonable expansion of state authority, while individual rights may be proportionally restricted. Consequently, citizens are obligated to accept and comply with the preventive measures implemented by administrative authorities [11].

The legal framework governing data disclosure in public health emergencies in China is dispersed across multiple legislative tiers, including constitutional provisions, statutory laws, and administrative regulations. While the Constitution of the People's Republic of China does not explicitly mandate governmental data disclosure, it implicitly guarantees citizens the right to participate in social governance and oversee state organs and officials. This, in turn, implies a right to access information and monitor public health emergencies. The Infectious Disease Prevention and Control Law, under Articles 19 and 38, vests national and provincial health administrative departments with the authority to release information on infectious diseases. Similarly, Articles 43 to 45 of the Emergency Response Law empower county-level and higher governments to disclose relevant emergency information to the public. Further statutory guidance is provided by the Regulations on the Disclosure of Government Information and the Regulations on Public Health Emergency Response, which impose affirmative duties on the government to release pertinent information.

Accordingly, China's legal framework for data openness in public health emergencies is structured as a hierarchical system. At its core, the Constitution serves as the foundational legal authority, supplemented by primary legislation such as the Emergency Response Law and the Infectious Disease Prevention and Control Law, while secondary regulations, including the Regulations on the Disclosure of Government Information and the Regulations on Public Health Emergency Response, provide specific implementation guidelines [12].

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3.2 Scope of Data Openness

Existing laws and regulations do not explicitly delineate the scope of data disclosure in public health emergencies. The Regulations on the Management of the Reporting and Disclosure of Infectious Diseases and Public Health Emergencies only reference data related to the nature, causes, location, scope, cases, casualties, response measures, and resolution of emergencies. While such data should undoubtedly fall within the scope of disclosure, evolving circumstances and practical needs necessitate a broader discussion on the openness of different data categories.

For personal data, the permissibility of disclosure largely depends on its sensitivity. Generally, the value of ordinary personal data is subordinate to public interest considerations, making its disclosure in public health emergencies justifiable when necessary to serve the public good. The critical issue lies in whether sensitive personal data can be disclosed and, if so, to what extent and through what mechanisms. Given that sensitive personal data is intrinsically linked to individual privacy, it falls within the realm of personal rights and requires heightened protection. Information that can directly identify individuals—such as names, identification numbers, and home addresses—should not be disclosed under ordinary circumstances [13]. Where disclosure is deemed essential for specific public health purposes, personal data should be anonymized or de-identified to prevent re-identification. For instance, during the COVID-19 outbreak in Changchun, Jilin Province, epidemic-related data was disclosed in an aggregated statistical format, revealing only affected areas while safeguarding individual privacy. This approach effectively balanced public health transparency with the protection of personal data.

The disclosure of epidemic-related public data requires government authorities to process and analyze collected data before making it accessible to the public or relevant stakeholders. The value of public data transparency lies in its potential for secondary processing and analytical applications. However, in some cases, complete de-identification may compromise the effectiveness of the data for public health purposes. Therefore, unless the data involves trade secrets, personal information posing a risk to public safety or social stability, or other legally protected interests, the guiding principle should be openness, with non-disclosure as the exception.

In public health emergencies, the government and government-led enterprises play a central role in data disclosure. While transparency in epidemiological investigations upholds the public's right to information, it may also inadvertently expose personal privacy. Thus, when disclosing such data, it is essential to ensure compliance with applicable legal and regulatory frameworks, prevent excessive disclosure, and implement robust anonymization measures. Moreover, public oversight mechanisms should be in place, granting citizens the right to challenge or seek redress if their data protection rights are infringed during the disclosure process. Prior to public release, authorities should also be obligated to notify affected individuals, thereby affording them an opportunity to understand and, where appropriate, contest the disclosure of their personal information.

For medical and health data, stricter technical safeguards and qualification review mechanisms should be established to regulate its development and application. When disclosing medical data within specialized

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

fields, careful attention must be given to defining data usage rights and implementing mechanisms for ensuring data integrity and withdrawal [14]. As for scientific research data, clear guidelines should be set regarding its confidentiality classification and retention period, with stringent controls over the conditions and methods of its publication to uphold the intellectual property rights of research institutions.

3.3 Principles of Epidemic-Related Data Openness

3.3.1 Principle of Efficiency

In the event of a public health emergency, the rapid spread of infectious diseases can pose severe threats to individuals' right to health and even their right to life. Under such circumstances, the government has a legal and moral obligation to disseminate relevant information promptly. Timely disclosure not only enables the public to take appropriate precautionary measures to safeguard lives and property but also mitigates public anxiety, prevents the spread of misinformation, and maintains social stability. The Emergency Response Law (Articles 7, 10, 20, 39, 40, 44, among others) underscores the necessity of promptly reporting emergencies to higher authorities and relevant agencies. Similarly, the Infectious Disease Prevention and Control Law mandates the timely release of information concerning the development of public health crises and emergency response measures, as stipulated in Article 4, Article 19, and Chapter 3, "Reporting, Notification, and Public Disclosure of Epidemics." Given the legal framework and the imperative of responding swiftly to public health emergencies, the principle of efficiency should serve as the foremost guiding principle in the disclosure of public health data.

3.3.2 Principle of Privacy Protection

During public health emergencies, certain restrictions on individuals' rights to personal information may be justified in the interest of public welfare. However, while public interest may, at times, take precedence over individual rights, it is essential to strike a careful balance and avoid disproportionately encroaching upon personal privacy. The publication of epidemic-related data must be conducted with due regard for privacy rights, ensuring that public safety considerations are assessed on a case-by-case basis. Even when disclosure involves individual information, personal privacy protections must be upheld. Wherever possible, only non-sensitive personal data should be released, or data should be anonymized prior to disclosure. Although emergency situations may necessitate temporary restrictions on certain rights, such restrictions must remain proportionate, necessary, and time-bound. Therefore, adherence to the principle of privacy protection is paramount when disclosing data related to public health emergencies.

3.3.3 Principle of Legality in Governmental Authority

Governmental actions, including the publication of data during public health emergencies, must be firmly grounded in legal authority. Both the entities responsible for data disclosure and the scope of such disclosures must be explicitly sanctioned by law. In China, statutes such as the Emergency Response Law, Infectious Disease Prevention and Control Law, Regulations on Government Information Disclosure, and Regulations on Emergency Response to Public Health Emergencies define the legal framework for data release. However, existing legal provisions remain insufficiently precise regarding key aspects such as the collec-

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

tion, storage, processing, disclosure, and deletion of data in public health emergencies. For instance, during epidemiological investigations, the absence of clearly defined responsibilities for data collection has led to a fragmented and complex system, increasing the risk of privacy violations. Similarly, ambiguous regulations on the subjects, methods, and scope of data disclosure have created legal uncertainties, potentially leading to infringements on personal privacy. To ensure that government agencies operate within a well-defined legal framework and uphold the rule of law, it is imperative to refine and enhance legislation governing data disclosure during public health crises.

4 Protection of Relevant Data in Public Health Emergencies

4.1 Legal Basis for Data Protection

Restrictions on personal information rights must strictly adhere to the principle of proportionality. As a fundamental doctrine in administrative law, the principle of proportionality mandates that any limitation on individual rights in the interest of public welfare must be both necessary and the least restrictive means available. In the context of public health emergencies, where the disclosure of personal or relevant data is unavoidable, measures should be taken to minimize harm, and sensitive personal data should not be disclosed unless absolutely essential. Even when disclosure is justified, data should be anonymized or pseudonymized to mitigate risks and protect individual privacy. While public interest is generally accorded priority over individual rights, this precedence is not absolute and must be assessed on a case-by-case basis [15]. Overemphasizing public interest must not come at the expense of fundamental personal rights and freedoms.

At the national legislative level, jurisdictions worldwide recognize the critical importance of data protection and have enacted comprehensive legal frameworks to safeguard personal information . These

statutes not only establish guidelines for the lawful processing of personal data but also provide a legal foundation for ensuring data security and regulatory compliance in the digital era. In China, personal data protection is embedded in multiple legislative instruments. For instance, Chapter 6 of the Civil Code enshrines the right to privacy and personal data protection; the Data Security Law introduces a regulatory framework for securing personal data; the Criminal Law contains provisions addressing unlawful data processing and breaches; and the Cybersecurity Law prescribes principles governing the collection, processing, and safeguarding of personal information by network operators. Additionally, legislation such as the Emergency Response Law, the Infectious Disease Prevention and Control Law, the Regulations on Government Information Disclosure, and the Regulations on Public Health Emergency Response not only provide the legal basis for data transparency during public health emergencies but also serve as critical safeguards for data protection.

4.2 Scope and Content of Data Protection

Personal data is generally categorized into general personal data and sensitive personal data, with data protection measures primarily concentrated on the latter. Sensitive personal data often contains highly pri-

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

vate information, some of which can directly identify individuals. During public health emergencies,widespread fear and panic can heighten public sensitivity to such data. The unauthorized disclosure of personal data related to infected individuals may severely disrupt their personal lives, compromise their reputations, and expose them to social discrimination. Accordingly, the protection of sensitive personal data must be given heightened attention in such circumstances. Public anxiety often leads to an excessive focus on individual cases, as exemplified by the widely publicized “Chengdu Girl” incident. Given these risks, safeguarding sensitive personal data during public health crises becomes a matter of paramount importance. Special emphasis must be placed on protecting PII, strengthening legislative frameworks for personal information protection in public health emergencies, and gradually establishing a liability-based punitive mechanism to enhance legal enforcement and compliance in data protection.

With respect to government data, transparency should serve as the guiding principle. However, caution must be exercised when handling data that involves trade secrets, personal privacy, or information that, if disclosed, could threaten social stability. The release of government data should adhere to the principles of legality, legitimacy, and necessity, ensuring that public interest data is classified and disclosed in a structured manner based on varying levels of sensitivity and access control [16]. Additionally, rigorous safeguards must be implemented to mitigate the risk of data breaches during storage. Such risks may arise from both internal and external threats: internal risks stem from inadequate oversight, weak internal control mechanisms, and potential insider misconduct, while external risks primarily involve cyberattacks and other forms of malicious exploitation. Regardless of the source, data breaches pose a significant threat, necessitating a robust and proactive approach to data security and risk management.

4.3 Principles of Data Protection

4.3.1Principle of Data Minimization and Purpose Limitation

China’s Emergency Response Law mandates that emergency measures prioritize the protection of citizens’ and organizations’ rights and interests. Article 6 of the Data Security Law explicitly stipulates that the processing of personal information must be conducted for clear and legitimate purposes, with data collection strictly limited to the minimum scope necessary to fulfill those purposes, thereby prohibiting excessive data collection. This legal framework firmly establishes the principles of data minimization and purpose limitation within national legislation.

Similarly, Article 9 of the EU General Data Protection Regulation (GDPR) imposes comparable restrictions on the processing of health-related data. China’s Personal Information Protection Law (PIPL) sets a robust legal standard for personal data protection, including the handling of data related to infectious diseases, aligning closely with the EU’s stringent regulatory framework [17]. In the context of public health emergencies, data collection and processing must be strictly confined to information essential for disease prevention and control. Any unrelated data collection should be avoided, and the methods employed must be both appropriate and proportionate, adhering to the principle of minimizing harm.

When partial disclosure of personal data is unavoidable, the least intrusive measures—such as anonymization or pseudonymization—should be implemented to mitigate risks to individual privacy. Moreover,

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

since public health emergencies inherently pose challenges to personal rights, it is essential to establish preemptive institutional mechanisms for legal redress and to strengthen post-crisis remedies for individuals whose rights may have been infringed [18].

4.3.2 Principle of Due Process

The principle of due process mandates that the collection, processing, and disclosure of data during public health emergencies adhere to legally established procedures, ensuring accountability throughout the entire data lifecycle—from collection to storage, processing, sharing, and ultimate deletion. This requirement serves as a safeguard to ensure that data controllers and processors comply with legal norms, particularly in exceptional circumstances where emergency measures may lead to an expansion of public authority and the exercise of extraordinary powers.

In such scenarios, reinforcing due process is critical to preventing potential abuses of power and ensuring that data protection standards are upheld, even in times of crisis. By maintaining procedural safeguards, governments and entities involved in emergency response can strike a necessary balance between safeguarding public health and upholding fundamental data protection rights.

5 Balancing Personal Information Protection and Public Interest in Public Health Emergencies

5.1 Clarifying the Data Collection Entities and Their Responsibilities

Laws and regulations such as the Emergency Response Law, the Infectious Disease Prevention and Control Law, the Government Information Disclosure Regulations, and the Emergency Response Regulations for Public Health Emergencies delineate the entities responsible for data collection during public health emergencies. These entities encompass a wide range of actors, including police stations, community offices, neighborhood committees, property management companies, and even non-governmental organizations like media outlets. While the diversity of these data collection entities facilitates the rapid and efficient gathering of epidemic-related data, it also substantially heightens the risk of privacy violations. Consequently, it is crucial for relevant laws and regulations to explicitly define the roles and responsibilities of these entities, establishing a framework for authorization and delegation to non-governmental actors. This framework should grant these entities the legal authority to collect personal information through lawful procedures and hold them accountable for any breaches of legal responsibility [19].

Data processors are legally obligated to implement adequate safeguards to protect the personal data they handle, ensuring data security while optimizing processing efficiency. This is essential to prevent incidents similar to the “Chengdu Girl” and “Yangzhou Grandma” cases, which highlight the consequences of data mishandling. Effective protection of personal information during public health emergencies requires not only a comprehensive legal framework but also robust organizational structures. Strengthening law enforcement agencies dedicated to personal information protection is a key responsibility of the government in this context. This necessitates that government departments take charge of drafting, formulating, and revising relevant regulations to safeguard personal data.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Government departments should clearly define their responsibilities in line with applicable laws, ensure proper allocation of duties, and enhance inter-agency collaboration during public health emergencies. On one hand, a standardized organizational structure must be established to ensure clear procedures and accountability throughout the stages of data collection, submission, processing, and analysis. On the other hand, given the unpredictable and urgent nature of public health emergencies, the organizational framework must remain flexible, enabling rapid adaptation to new challenges. Public health emergencies place significant demands on the government's capacity to protect personal information, necessitating improvements in governance. These improvements should include strengthening personal information protection agencies and enhancing the awareness and capabilities of government personnel to address the evolving challenges presented by the era of big data.

5.2 De-identification of Personal Data

Identifiability serves as the key criterion for determining whether data qualifies as sensitive or whether its disclosure could infringe upon an individual's rights. In the context of public health emergencies, the public interest often necessitates the relinquishment of certain individual rights, which may include the disclosure of personal data. However, to balance the protection of personal privacy with the fulfillment of public health objectives, data must undergo a process of "de-identification." This process involves anonymizing or pseudonymizing the data prior to disclosure, thereby reducing the potential risks to individuals. During de-identification, a case-by-case approach should be employed, with differentiated anonymization standards based on factors such as the type of medical information controller, the scope of data disclosure, the sensitivity of the information, and the likelihood of re-identification [20]. This approach ensures that the public's right to information is upheld, while simultaneously minimizing the intrusion into individual privacy and safeguarding personal data rights.

5.3 Right to Be Forgotten

Upon the conclusion of a public health emergency, the substantial amounts of personal data collected during the response must be disposed of appropriately. Pursuant to Article 47 of the Personal Information Protection Law, data controllers are obligated to delete personal data once the processing purpose has been fulfilled. Similarly, the "right to be forgotten," enshrined in Article 17 of the EU GDPR, is designed to curb the excessive retention and use of personal data [21]. This right is rooted in the principle of human dignity, advocating for the protection of individuals' identities and interests. In the context of public health emergencies, individuals may be required to disclose certain personal information to safeguard public health. However, once the emergency has subsided and the data processing purpose has been achieved, the collected data must be erased or destroyed to prevent unauthorized use and to safeguard individuals' privacy.

The exercise of the right to be forgotten may conflict with competing interests, and thus, its scope requires further clarification. During the active phase of a public health emergency, data collected for purposes of public health, social stability, or other public interests should not be subject to the right to be forgotten. However, if individual rights are infringed, the affected party may seek civil remedies from the data processor pursuant to Article 995 of the Civil Code. Should actual harm result from the misuse of data, the data processor may also be liable for compensation.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

5.4 Strengthening Cybersecurity and Legal Frameworks in Health Data Protection

As digital health technologies continue to evolve, it becomes increasingly critical to implement robust cybersecurity measures and establish a clear and comprehensive legal framework that effectively balances the protection of personal information with the broader public interest. The widespread adoption of Internet of Things (IoT) devices in healthcare introduces new complexities in safeguarding sensitive personal data against cyber threats. Existing regulatory frameworks must be adapted to address these emerging risks while ensuring compliance with data protection laws[22].Furthermore, regulatory approaches to health data governance must carefully balance the objectives of information sharing with the protection of privacy.The legal challenges surrounding public health orders and digital health surveillance also warrant significant attention.To effectively address these challenges, an integrated approach is essential—one that includes updating cybersecurity regulations, refining legal frameworks for health data governance, and ensuring that emerging technologies comply with established data protection principles.[23] By strengthening these measures, governments can better protect personal information while maintaining their capacity to respond effectively to public health crises [24].

6 Conclusion

Data governance in public health emergencies represents a complex and urgent challenge. The occurrence of such crises underscores the pivotal role of big data technology in epidemic prevention and control within the context of digital governance. This paper examines the necessity and significance of big data in public health emergencies and delves into data governance issues from the perspectives of data openness and protection by analyzing and defining data rights.

While the deployment of big data presents innovative solutions for managing public health emergencies, it simultaneously introduces new challenges, particularly in terms of balancing data openness with the protection of personal privacy. Striking a balance between safeguarding individual privacy and serving the broader public interest is essential. This requires a collaborative effort from governments, research institutions, businesses, and the public to establish appropriate data governance policies and practices. Only by implementing a well-structured data openness and protection framework can we effectively respond to public health emergencies and safeguard the health and safety of the public.

References

[1] Zhao, H: Legal Regulation of Cross-border Data Flow and National Security: Challenges and Responses [EB/OL].2024-09-23.https://law.cnr.cn/fzjj/20240923/t20240923_526915139.shtml

[2] Li, Y., Kuai, L., & Zhang, A. (2024). Research on the System of Big Data in Science and Technology Government Affairs for the Digitalization of Government Services. Jiangsu Science and Technology Information, 14, 67-70.

[3] Wang, L. (2022). Basic Issues in the Protection of Sensitive Personal Information: Background of the Interpretation of the Civil Code and Personal Information Protection Law. Contemporary Jurisprudence, 01, 3-14.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

[4] Hong, L. (2022). On the Use and Protection of Personal Information in Epidemic Prevention and Control. Local Legislation Studies, 04, 49-59.
[5] Song, H. (2018). The Development and Construction of the Legal System for Government Data Disclosure in China. Administrative Law Studies, 02, 35-46.
[6] Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Data Infrastructure System to Better Leverage the Role of Data as a Factor of Production/OL.2022-12-19. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm
[7] Hong, L. (2022). On the Use and Protection of Personal Information in Epidemic Prevention and Control. Local Legislation Studies, 04, 49-59.
[8] Xu, K. (2024). Theoretical Reinterpretation of Personal Information Rights: The Rights Tree. Gansu Social Sciences, 02, 139-150. doi:10.15891/j.cnki.cn62-1093/c.20240409.004.
[9] Xu, K. (2024). The rights tree: A theoretical reinterpretation of personal information rights. Gansu Social Sciences, 2, 139-150. https://doi.org/10.15891/j.cnki.cn62-1093/c.20240409.004
[10] Karanicolas, M. (2021). Even in a Pandemic, Sunlight Is the Best Disinfectant: COVID-19 and Global Freedom of Expression. Oregon Review of International Law, 22, 1-22.
[11] Gao, Z. (2022) . Public Interest Considerations in Personal Information Protection: A Perspective on Responding to Public Health Emergencies. East Law Journal, 03, 17-32. doi:10.19404/j.cnki.dffx.20220424.005.
[12] Zhou, W. (2021). On the Legal Regulation of Information Disclosure in Public Health Emergencies: Including Suggestions for Revising Article 38 of the Infectious Disease Prevention and Control Law. Administrative Law Studies, 04, 147-161.
[13] Kong, F. (2020). Protection of Personal Privacy in Government Information Disclosure. Administrative Law Studies, 01, 17-29.
[14] Zhang, Y. (2023). Interpretation and Legal Breakdown of Major Epidemic Data in the Digital Government Era. Decision Science, 01, 60-69.
[15] Ning, Y. (2020). Regulation of Personal Information Protection in Health Code Applications. Legal Studies Review, 06, 111-121. doi:10.13415/j.cnki.fxpl.2020.06.012.
[16] Yin, J., Zhou, C. (2024). On the Reasonable Use of Personal Information in Government Data Openings. Journal of Shanxi University (Philosophy and Social Science Edition), 02, 38-48. doi:10.13451/j.cnki.shanxi.univ (phil.soc.).2024.02.005.
[17] Xu, F. (2022). The Establishment and Maintenance of Network Sovereignty and Data Sovereignty. Beijing Social Science, 07, 55-64. doi:10.13262/j.bjsshkxy.bjshkx.220706.
[18] Wang, Q. (2020). Legal Principles and Legal Thinking in Responding to Public Health Emergencies. Law and Society Development, 03, 65-77.
[19] Zheng, Y. (2024). A Study on the Legalization of Personal Information Collection in Public Health Emergencies. Journal of Northeastern University (Social Science Edition), 05, 100-108. doi:10.15936/j.cnki.1008-3758.2024.05.011.
[20] Kaplan, B. (2015). Selling Health Data: De-identification, Privacy, and Speech. Cambridge Quarterly of Healthcare Ethics, 24 (3), 256-271.
[21] Rizzuti, M. (2020). Gdpr and the Right to be Forgotten. European Journal of Privacy Law & Technologies (EJPLT), 2020 (Special Issue), 105-112.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

[22] Casarosa, F. (2024). Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. Computer Law & Security Review, 49, 105982. https://doi.org/10.1016/j.clsr.2024.105982
[23] Kenny M.& Eric A. Posner (2022), Constitutional Challenges to Public Health Orders in Federal Courts During the Covid-19 Pandemic, Boston University Law Review,1729 .
[24] Michael L. Cederblom (2022), Welcome to the Digital Age: Reinventing Contact Tracing and the Public Health Service Act for A Modern Pandemic Response, Annals of Health Law,101.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)