A Study on Medical Data Privacy Protection and Solutions: A Perspective on the Protection of Minors' Privacy

Shixin Fan
School of Law, Xinjiang University of Finance and Economics, Urumqi, Xinjiang, China

Abstract: Against the backdrop of the widespread adoption of digital healthcare, the shortcomings in the protection of minors' medical data—a particularly sensitive category of information that combines personal attributes with public value—are becoming increasingly apparent. Given that minors are physically and psychologically immature and have limited ability to assess risks, their medical data encompasses sensitive information spanning the entire life cycle, including vaccination records, medical histories, genetic testing results, and mental health records. Should such data be leaked, misused, or commercialized in violation of regulations, it could easily lead to irreversible consequences such as personal discrimination and infringement of rights. Although China has established a foundational protective framework through the Personal Information Protection Law, the Law on the Protection of Minors, and the Civil Code, practical challenges—such as fragmented regulations in medical settings, the erosion of informed consent, ambiguous regulatory responsibilities, and insufficient adaptation to the needs of special groups—remain unresolved. Consequently, the conflict between the value of utilizing medical data and the need for privacy protection continues to intensify. This paper focuses on the unique characteristics of minors' medical data, delves into practical challenges, synthesizes international experiences, and derives localized insights. It emphasizes systematic solutions to these challenges. The research is grounded in empirical research, contains no fictional content, and meets the publication standards of core legal journals.

Keywords: Medical Data; Privacy Protection; Minors; Sensitive Personal Information; Informed Consent; Legal Regulation

1. Introduction

With the deep integration of digital healthcare and big data, medical data has become a critical resource for diagnosis and treatment, scientific research, and public health prevention and control, and the scope of collection and use of minors' medical data continues to expand [1-4]. Such data spans the entire developmental cycle of minors; it is highly sensitive and has lifelong implications. Any leakage, misuse, or illegal commercialization of this data would severely infringe upon their personal dignity and right to privacy, and could also lead to long-term discrimination in areas such as education, employment, and insurance, causing irreversible harm [5,6]. Chinese legislation has classified health and medical data as sensitive personal information and established principles such as guardian consent and data minimization; however, specialized protections for minors' medical data remain inadequate. In practice, issues such as the formalization of informed consent, non-compliant data processing, weak oversight, and difficulties in asserting rights are prominent, making it difficult to achieve the legislative goal of providing preferential protection [7]. Compared to adults, the unique characteristics of minors' medical data have not received sufficient attention, and a mechanism to balance data utilization with privacy security has yet to be established [8]. Therefore, this paper focuses on the privacy protection of minors' medical data, analyzes its unique characteristics and current challenges, draws on international experiences, and proposes practical improvement strategies to provide guidance for improving relevant legal systems and strengthening the protection of minors' medical privacy [9].

2. Defining the Unique Characteristics of Medical Data Privacy Protection for Minors

Medical data pertaining to minors is not ordinary personal information; rather, it constitutes special and sensitive information that combines

both privacy rights and personal information rights. Given the unique nature of its subjects, content, and the exercise of rights, conventional medical information protection rules are insufficient to fully address these issues. Consequently, a differentiated and robust protection model must be adopted, which serves as the logical starting point for this study [10].

2.1 Characteristics of the Target Group: Vulnerable Status and Lack of Risk Awareness

Minors are classified as individuals with no or limited capacity for civil conduct. As their physical and mental development is not yet fully mature, they lack a basic understanding of the value of medical data, the risks of data breaches, and the consequences of infringement. Consequently, they are unable to independently assess the legality of data processing activities or exercise their rights—such as the right to access, correct, delete, or withdraw consent—and must rely entirely on their guardians to act on their behalf to protect their rights [11]. However, guardians often lack specialized knowledge regarding the protection of medical data, which can lead to issues such as blind consent and lax supervision. In some cases, there may even be instances of abuse of guardianship or unauthorized disposal of minors' medical data, further amplifying the risk of rights violations [12]. Compared to adults, minors lack the capacity and channels to defend their own rights. Faced with the dominant position of data processors, their rights are easily overlooked or even infringed upon; this is the core reason why the law must provide them with preferential protection [13].

2.2 Unique Characteristics of Data: Highly Sensitive and Linked for Life

Medical data on minors encompasses core information such as physiological indicators, medical histories, genetic information, mental health status, and history of infectious diseases. It falls under the highest category of sensitive personal information as defined by the *Personal Information Protection Law*, and certain confidential data is also strictly protected under privacy rights [2]. Such data not only concerns the safety of current medical treatment but also has lifelong implications. Once information regarding genetic defects, mental illnesses, or a history of infectious diseases is leaked, it creates a permanent stain on one's privacy, easily leading to social discrimination. This directly impacts minors' core rights and interests in areas such as future education, employment, and romantic relationships, with consequences that are covert, long-term, and irreversible [6]. In particular, genetic data and mental health treatment records not only concern the minors themselves but may also involve family privacy; once leaked, they pose risks of a broader scope and deeper harm [14].

2.3 Special Characteristics of the Exercise of Rights: Dual Agency and Conflicts of Interest

The exercise of rights regarding minors' medical data involves a two-tiered agency structure comprising "minor—guardian—data processor." Although guardians serve as legal representatives, their wishes may not always fully align with the minor's best interests [7]. In practice, unilateral consent by guardians often supersedes the minor's own wishes, particularly in the case of adolescents aged 14 and older who possess a certain level of cognitive ability, whose autonomy regarding medical privacy is completely disregarded. At the same time, medical data involves both private rights and public interests; the data utilization needs of research institutions and medical facilities frequently conflict with minors' privacy protection demands, making the balancing of these interests far more challenging than with ordinary personal information [8]. Finding a balance between guardian representation, data utilization, and the autonomous will of minors has become the core challenge in the protection of medical data privacy [9].

3. Practical Challenges in Protecting the Privacy of Minors' Medical Data

Currently, China has yet to establish a comprehensive system for the protection of minors' medical data; there are significant shortcomings in legislation, practice, regulation, and remedies, making it difficult to implement the specific requirements for protecting this vulnerable group. These challenges are primarily manifested in four key areas.

3.1 Fragmented Legislative Rules and Superficial Special Protections

Regulations governing the protection of minors' medical data are scattered across multiple laws and regulations, providing only general

principles and lacking specific implementation rules tailored to medical contexts, resulting in a situation characterized by "broad protection but insufficient specificity" [11]. There is no distinction between data sensitivity levels, resulting in an imbalance in the level of protection between highly sensitive data and ordinary clinical data; the criteria for guardian consent are vague, and the boundaries of autonomous consent for minors aged 14–18 remain undefined; there are no explicit prohibitions on core processes such as data storage, sharing, and commercialization; and new issues such as cross-border data transfers and re-identification after de-identification lack regulation, with legislation lagging behind the pace of digital healthcare development [12].

3.2 The Principle of Informed Consent Has Been Eroded, and Formalism Is a Prominent Issue

Informed consent serves as the legal basis for the processing of medical data, but in practice, it has been severely undermined [1]. The information provided is often obscure and verbose, making it difficult for guardians to understand key details regarding data collection, use, and sharing; "blanket consent" is widespread, with authorization for clinical data bundled together with authorization for research and commercial data, leaving guardians with no right to refuse specific uses; there is a lack of a dynamic consent mechanism, making it impossible to monitor data flows, and channels for withdrawal or deletion are blocked, completely excluding minors' autonomous will and leaving the authenticity and voluntariness of consent unguaranteed [3].

3.3 Non-Standard Data Processing and Significant Security Risks Throughout the Entire Process

Compliance breaches occur frequently throughout the entire data processing workflow: during the collection phase, unnecessary information is collected beyond the required scope, violating the principle of data minimization [4]; during the storage phase, primary healthcare institutions suffer from outdated encryption technologies and lax access controls, resulting in a high risk of internal leaks [5]; during the sharing phase, anonymization techniques are misused, allowing individuals to be re-identified after data aggregation [7]; and during the destruction phase, statutory retention periods are not strictly enforced, with widespread instances of data being retained beyond the permitted timeframes and disposed of arbitrarily, further amplifying the risk of leaks [8].

3.4 Regulatory Remedies Are Slow to Materialize, and the Protection of Rights and Interests Is Inadequate

At the regulatory level, there is an overlap of responsibilities among multiple departments, resulting in regulatory gaps. There is a lack of routine collaborative law enforcement and specialized ethical reviews, and penalties for violations are too lenient to serve as an effective deterrent [9]. At the redress level, rights protection faces challenges in proving liability, obtaining a ruling, and securing compensation, and the burden of proof has not been shifted to the defendant [10]; the threshold for compensation for emotional distress is high, the scope of public interest litigation is narrow, organizations dedicated to protecting minors lack the authority to intervene, and the cost of seeking redress is extremely high, making it difficult to hold perpetrators accountable in most infringement cases [11].

4. Lessons Learned from Overseas Practices on the Protection of Minors' Medical Data Privacy

Countries and regions with an early start in the development of global digital healthcare have all established systematic legal frameworks and practical mechanisms tailored to the unique nature of minors' medical data. Through specialized legislation, tiered protection, strict oversight, and diverse remedies, they strike a balance between data utilization and privacy protection; their proven experience offers valuable lessons for China [12].

4.1 Germany: Comprehensive Protection of Rights + Reversal of the Burden of Proof

As a representative of the civil law system, Germany has established detailed rules for the protection of minors' medical data under the EU's GDPR framework, in conjunction with its own Federal Data Protection Act and Medical Code, placing particular emphasis on substantive informed consent and remedies for infringements [1]. German law explicitly stipulates that minors' rights to consent to

medical treatment and to data disclosure must be differentiated based on age group and treatment risk. For low-risk routine treatments, minors aged 14 and older may express their opinions, while high-risk treatments require full consent from the guardian; When fulfilling their duty to inform, healthcare institutions must use language understandable to both guardians and minors, clearly outline data risks and avenues for redress in writing, and strictly prohibit the misuse of standard form clauses [2,3]. Regarding the determination of liability for infringement, Germany implements a reversal of the burden of proof: in the event of a breach of a minor's medical data, the data processor must prove its own lack of fault; otherwise, it bears full liability for compensation, significantly reducing the difficulty for victims to seek redress [4]. Additionally, Germany has established an independent data protection supervisory authority specifically responsible for overseeing compliance with medical data regulations. This authority can impose penalties such as orders to rectify violations, suspension of operations, and substantial fines, demonstrating a high degree of regulatory independence and expertise [5].

4.2 Japan: Multi-Stakeholder Collaboration + Child-Friendly Protection

Based on the Personal Information Protection Act, Japan has established a three-party collaborative mechanism involving the government, medical institutions, and families to manage minors' medical data, emphasizing child-friendliness and practicality [6]. Japanese law requires that the processing of minors' medical data must adhere to the principles of "minimum necessity" and "purpose limitation"; it prohibits the collection of information unrelated to medical treatment, and stipulates that data retention must not exceed the period necessary for medical care[7]; When obtaining consent from guardians, medical institutions must use "child-friendly" methods—such as simplified consent forms and illustrated explanations—to ensure guardians quickly grasp the key points. Additionally, for minors with the capacity to understand, they must be informed simultaneously and their wishes must be heard [8]. At the regulatory level, Japan has established the Personal Information Protection Commission to oversee medical data regulation and has created mechanisms for reporting violations and rapid resolution [9]; In terms of remedies, the scope of entities eligible to file public interest lawsuits has been expanded to allow associations for the protection of minors and consumer groups to file lawsuits on behalf of affected parties, thereby lowering the threshold for seeking redress [10]. Furthermore, Japan emphasizes public education on privacy protection, conducting outreach through schools and communities to enhance risk prevention awareness among guardians and minors, thereby achieving a combination of legal regulation and social co-governance [11].

4.3 Summary of Common Features in International Experiences and Implications for Localization

Based on the experiences of the jurisdictions mentioned above, a clear common logic emerges regarding the protection of minors' medical data in foreign jurisdictions: First, prioritize protective measures by classifying minors' medical data as the highest level of sensitive information and establishing protection standards that are stricter than those for adults [12]; second, implement tiered and categorized regulations by differentiating rules based on age, data sensitivity, and usage scenarios, balancing protection with efficiency [13]; third, strengthening substantive informed consent by rejecting formalism and ensuring that consent is genuine and voluntary [1]; fourth, establishing an independent regulatory framework coupled with strict disciplinary mechanisms to increase the cost of non-compliance [2]; Fifth, improving accessible remedies by lowering the threshold for rights protection and implementing a reversal of the burden of proof [3]. These experiences cannot be applied wholesale; China must adapt them to local conditions by integrating them with its domestic legislative framework and the current state of its healthcare system, drawing on the essence of these practices. The focus should be on adopting core mechanisms such as tiered consent, privacy by design, regulatory coordination, and optimized remedies to address the shortcomings of the existing system [4, 5].

5. Key Approaches to Protecting the Privacy of Minors' Medical Data

To address the challenges surrounding the protection of minors' medical data privacy, we must recognize their unique circumstances and adhere to the core principle of "the best interests

of the child." By building on detailed legislation as a foundation, leveraging technological capabilities as support, ensuring regulatory coordination as a safeguard, and establishing robust remedies as a safety net—while drawing on proven international practices—we can construct a comprehensive, systematic protection framework. Key measures should be implemented across five key dimensions [6,7].

5.1 Legislative Refinement: Establishing Tiered and Categorized Special Protection Rules

To address the issue of fragmented legislation, specific and detailed rules should be established for minors' medical data to ensure targeted protection [8]. First, establish a three-tiered consent mechanism that differentiates consent rules based on age and cognitive ability: for those aged 0–12, consent is granted solely by the guardian; for those aged 13–17, consent is granted jointly by the guardian and the minor; for low-risk medical data, the minor's autonomous will is fully respected; and for those aged 18 and above, consent is granted entirely autonomously; Mandatorily implement "child-friendly" disclosure obligations, using plain language, illustrations, and audio to simplify disclosure content and eliminate obscure standard-form clauses [9]. Second, implement tiered classification and protection of data, categorizing minors' medical data into three levels: highly sensitive (genetic, psychiatric treatment, and infectious disease history), moderately sensitive (routine medical history), and low-sensitivity (basic physical examinations). Commercial use of highly sensitive data is strictly prohibited; collection is permitted only when medically necessary and requires separate written consent. Moderately sensitive data is restricted to use within the scope of medical treatment. Low-sensitivity data may be subject to presumed consent, with an opt-out option provided [10]. Third, establish clear red lines for data processing, strictly enforce the principle of data minimization, standardize storage periods and destruction procedures, prohibit illegal cross-border transfers and commercial exploitation, and supplement prohibitions against the re-identification of de-identified data to curb non-compliant processing at the source [11].

5.2 Substantive Optimization: Restructuring the Core Rules of Informed Consent

We must move away from formalism and restore informed consent to its essence as a "genuine expression of intent" [1]. First, consent modules should be separated, with distinct authorizations for data required for diagnosis and treatment, data used for research, and data used for commercial purposes. Guardians should be allowed to refuse non-essential authorizations individually, thereby eliminating "blanket consent" [2]. Second, clarify the core elements of disclosure: medical institutions must provide written disclosure of the scope of data collection, purpose of use, recipients of shared data, storage period, risks of leakage, and avenues for redress. Key clauses should be highlighted in bold to ensure guardians fully understand the terms before signing [3]. Third, establish a dynamic consent mechanism by creating an online inquiry platform that allows guardians to view data flows in real time, supports one-click withdrawal of consent and requests for data deletion, and requires reauthorization for any changes in data processing practices [4]. Fourth, incorporate the wishes of minors. For minors aged 14 or older who possess cognitive capacity, medical data processing must fully take their opinions into account; their reasonable wishes must not be forcibly disregarded, thereby balancing parental authority with the minor's autonomy [5].

5.3 Technical Safeguards: Establishing a Robust Data Security Barrier Throughout the Entire Process

Use technological measures to address management gaps and ensure that minors' medical data is "accessible yet invisible, controllable yet traceable" [6]. On the one hand, privacy-enhancing technologies should be promoted, with the comprehensive application of differential privacy, federated learning, and dynamic anonymization techniques. For research and data sharing, only de-identified data should be provided, and the leakage of raw data must be strictly prohibited. A tiered access control system should be established, with access to highly sensitive data authorized only for core medical staff; all access and operational activities must be fully logged and traceable [7]. On the other hand, improve security assessment mechanisms: healthcare institutions must conduct specialized security impact assessments before processing minors' medical data and

regularly identify technical vulnerabilities; develop data breach contingency plans to immediately activate response procedures upon any breach, promptly notify guardians and regulatory authorities, and minimize the consequences of harm to the greatest extent possible [8]. At the same time, drawing on the EU's "privacy-by-design" principle, require medical data systems to embed security protection features during the R&D phase to achieve preventive control [9].

5.4 Regulatory Coordination: Establishing a Multi-Stakeholder Regulatory Framework

Break down barriers to fragmented regulation and establish a specialized, routine regulatory synergy [10]. First, clarify regulatory responsibilities: the health department should take the lead in establishing a special regulatory task force in collaboration with the Cyberspace Administration and the Market Regulation Bureau. This task force will be specifically responsible for compliance inspections of minors' medical data, complaint handling, and penalties for violations, thereby clarifying the boundaries of each department's responsibilities and eliminating regulatory gaps [11]. Second, strengthen end-to-end oversight by establishing mechanisms for pre-processing ethical review, routine monitoring during operations, and post-incident accountability and disciplinary action. Conduct regular compliance inspections of medical institutions and data processing companies, increase fines for illegal collection, disclosure, and commercialization of data, and raise the cost of non-compliance by benchmarking against international standards [12]. Third, promote industry self-regulation by guiding medical institutions to formulate a self-regulatory code of conduct for the protection of minors' medical data, establish the position of privacy officer, strengthen privacy protection training for medical staff, and reinforce professional ethical constraints; facilitate public reporting channels, encourage oversight by the public and the media, and establish a multi-stakeholder governance system comprising government regulation, industry self-regulation, and social oversight [13].

5.5 Improving Remedies: Lowering the Threshold for Seeking Redress and Strengthening Safeguards for Rights

Addressing challenges in rights protection and establishing a convenient and efficient redress system [14]. First, implement a reversal of the burden of proof. Drawing on Germany's legislative experience, data processors should bear the burden of proving the legality and lack of fault in their processing activities, thereby reducing the evidentiary burden on minors and their guardians [1]. Second, expand the scope of entities eligible to file public interest lawsuits by granting such standing to organizations dedicated to the protection of minors and consumer associations, enabling them to pursue collective redress against mass infringements [2]. Third, improve the compensation mechanism by clarifying standards for compensation for emotional distress and including damages for privacy violations and potential risks of discrimination within the scope of compensation; introduce punitive damages for intentional data leaks or misuse resulting in severe consequences to increase the cost of infringement [3]. Fourth, streamline the rights protection process by establishing dedicated service windows and online channels to provide free legal consultation and legal aid to minors and their guardians, thereby bridging the "last mile" in rights protection [4].

6. Conclusion

The protection of minors' medical data privacy is a core issue at the intersection of personal data protection and the safeguarding of minors' rights. Given the vulnerability of the data subjects, the highly sensitive nature of the data, and the complexity of exercising rights, it is imperative to abandon generalized protection models and implement precise, stringent special regulations. The challenges currently facing China—including fragmented legislation, the erosion of informed consent, regulatory lag, and inadequate remedies—are fundamentally the result of a lack of special protection rules and the failure of interest-balancing mechanisms. Meanwhile, the experiences of foreign jurisdictions such as the European Union, the United States, Germany, and Japan—including tiered protection, substantive consent, and strict regulation—provide important references for improving China's institutional framework.

To address these challenges, the key lies in closely addressing the unique nature of minors' medical data, drawing on mature international experiences while grounded in China's national conditions. This approach should be based on

legislation that refines tiered and categorized protection rules, reconstructs a substantive informed consent mechanism, builds robust security defenses through technology, strengthens regulatory constraints through collaborative oversight, and safeguards rights through comprehensive remedies. Ultimately, this will achieve a dynamic balance between the reasonable use of medical data and the protection of minors' privacy. In the future, we must continue to monitor emerging scenarios and issues in digital healthcare, continuously refine regulatory details, and strengthen the implementation of law enforcement and judicial proceedings. This will ensure that the legislative intent of providing preferential protection is truly translated into practical results, thereby building a solid digital privacy defense for the healthy growth of minors.

References

[1] Guo Yuanyuan. A Study on Civil Liability for Violations of Patients' Right to Informed Consent. Lanzhou University, 2020.

[2] Yang Zaihui. Private Law Protection of Medical Genetic Information in the Era of the Civil Code. Chinese Health Services Management, 2021, 38(11):845-848.

[3] Wang Xiaoyu. A Study on Consent Rules for the Protection of Personal Medical Information under Scenario Theory. Jiangnan University, 2025.

[4] Xu Huili. Legal Protection of Personal Medical Information in the Big Data Environment. Library, 2019(11):45-51.

[5] Yu Wenjuan. A Study on the Civil Law Protection of Personal Health Information in the Digital Age. Jilin University, 2022.

[6] Hu Xinyue. A Study on Legal Issues Regarding Medical Consent for Minors. East China University of Political Science and Law, 2023.

[7] Hong Xinlin. Legal Protection of Citizens' Personal Medical Data in China. Anhui University, 2022.

[8] Chen Na. A Study on the Legal Protection of Patient Privacy in the Era of Healthcare Big Data. Southwest University of Political Science and Law, 2021.

[9] Sun Hui. Classification of the Legal Nature of Medical and Health Information and Its Protection under Private Law. Graduate School of the Chinese Academy of Social Sciences, 2020.

[10] Zhao Wenyi. A Study on the Civil Law Protection of Patients' Rights to Personal Information in the Sharing of Medical Data. Minzu University of China, 2023.

[11] Zhang Xinbao. Commentary on the Personal Information Protection Law of the People's Republic of China. Beijing: China Law Press, 2021.

[12] Cheng Xiao. Understanding and Application of the Personal Information Protection Law. Beijing: China Legal Publishing House, 2021.

[13] He Yan. On the Legal Protection of the Right to Privacy of Personal Medical Information. Sichuan University, 2020.

[14] Shen Wei. A Study on Exceptions to the Duty of Medical Confidentiality. Southwest Medical University, 2021.

