

Legal Mechanisms for Protecting Children's Personal Health Data in the Implementation of Sickness Insurance Benefits in Vietnam: Current Practice and Directions for Legal Education

Nguyen The Mung^{1*}, Nguyen Thi Thao²

¹Electric Power University, Vietnam Email: mungnt@epu.edu.vn; Orcid: 0009-0001-4989-5728

Email: thaont9@epu.edu.vn; Orcid: 0009-0008-8378-9436

²Electric Power University, Vietnam Email: thaont9@epu.edu.vn; Orcid: 0009-0008-8378-9436

HOW TO CITE:

Nguyen The Mung, Nguyen Thi Thao (2026). Legal Mechanisms for Protecting Children's Personal Health Data in the Implementation of Sickness Insurance Benefits in Vietnam: Current Practice and Directions for Legal Education. International Journal of Special Education, 41(9s), 907-932

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.

Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY)

license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

On the basis of an analysis of legal provisions on social insurance, personal data protection, and children's rights, combined with an assessment of the practical procedure for settling sickness benefits, the article shows that risks to children's health data arise not only from limitations in the legal framework but also from the design of administrative procedures, the data-security capacity of actors involved in data processing, and the legal awareness of parents or guardians. From this perspective, the article argues that the protection of children's health data in the implementation of sickness benefits must be approached comprehensively, combining legal reform, strengthened technical safeguards, and enhanced legal education. The proposed solutions include improving the data-confidentiality responsibilities of healthcare personnel, training human resources officers and social insurance officers on the principle of data minimisation, strengthening parents' awareness of children's digital privacy, and integrating personal data protection principles from the design stage of forms and information systems used for the settlement of social insurance benefits. On that basis, the article affirms that safeguarding children's right to personal data protection is an important condition for ensuring that modernisation and digital transformation in the field of social security are implemented in a sustainable, humane manner and in conformity with standards for the protection of children's rights.

Keywords: sensitive personal data; children's privacy; sickness insurance; health data; data ethics; legal education.

1. Introduction

Digital transformation in healthcare and social insurance is reshaping how personal data are collected, stored, and used. The introduction of electronic health records, the VssID application,

the social insurance database, and the Electronic Health Book integrated into VNeID has simplified administrative procedures and improved the settlement of social insurance entitlements, including sickness benefits. Under guidance issued by the Ministry of Health, health

data that are interoperable and fully displayed on VNeID may be used in place of the corresponding medical documents in administrative procedures. Yet when health data, particularly children's health data, are shared and processed by multiple actors in the course of benefit settlement, the risk of privacy infringement increases. This creates a pressing need to improve the legal mechanism for safeguarding children's privacy, dignity, and best interests in the digital environment. This question becomes particularly acute in the procedure for resolving social insurance benefits when an employee takes leave to care for a sick child under seven years of age. In substance, this is a necessary social security policy, reflecting the responsibility of the state to protect families, children, and workers. For that entitlement to be implemented, however, information about the child's medical condition must pass through several different actors. The healthcare facility issues the certificate of leave for social insurance benefits. The parent submits that certificate to the enterprise. The human resources or accounting department verifies, retains, digitises, and forwards the dossier to the social insurance agency. Children's health data, therefore, do not remain confined to the relationship between the patient and the healthcare provider. They are introduced into an administrative processing chain involving non-medical intermediary actors.

The sensitivity lies precisely in this movement. Information concerning a child's health status is directly connected to private life, honour, dignity, and the risk of social stigma. Once such data are received by an employer or an enterprise's human resources staff, the purpose of processing is no longer medical examination or treatment, but the verification of eligibility for a social security benefit. This change of purpose is not automatically unlawful. It does, however, require a more stringent data protection mechanism than that applied to ordinary administrative forms. If the procedure focuses only on the formal validity of the dossier without examining the scope of necessary data, the retention period, internal access rights, confidentiality obligations,

and deletion mechanisms after the processing purpose has been fulfilled, a social security entitlement may inadvertently be realised in a manner that heightens risks to children's privacy. From a legislative perspective, this is not an isolated defect of a single procedure. It reflects the inevitable lag of legal regulatory techniques behind the pace of digitalisation. Social insurance law is designed primarily to determine eligibility conditions, benefit levels, and payment procedures. Health law focuses on medical examination and treatment, professional standards, and the management of medical records. Personal data protection law has only recently emerged as an independent regulatory framework, with principles governing purpose limitation, the protection of data subjects, the protection of children's data, and the protection of data in the health sector. When these three fields intersect in a concrete procedure, the coordination gap becomes visible. The problem is not that the legal system wholly lacks protective rules. It is that existing provisions have not yet been fully translated into operational standards for each link in the sickness insurance process.

The issue becomes even more complex when viewed through the actual behaviour of the actors involved. Parents often prioritise the completion of the dossier in order to receive the allowance and therefore have little practical opportunity to consider their child's data privacy. Enterprises may treat the certificate of leave for social insurance benefits as an ordinary labour-related document rather than as a record containing sensitive health data. Healthcare facilities, although bound by the duty to maintain patient confidentiality, must still issue certificates according to a uniform administrative template. Social insurance agencies need data to verify that payments are made to the right beneficiaries under the correct regime, yet they must also ensure that data processing does not exceed what is necessary. For that reason, the risk of data infringement in this context does not arise from a single point of failure. It is formed across the entire data life cycle, from creation, transfer, receipt, storage, and use to deletion or continued

retention after the procedure has ended.

Meanwhile, current studies on personal data protection in Vietnam tend to focus on e-commerce, social networks, cybersecurity, or data governance in general. The flow of children's health data in the procedure for claiming sickness insurance benefits has not yet been analysed as an independent legal issue. This gap has considerable scholarly and policy significance. It shows that personal data protection cannot be discussed only at the level of general principles. It must be tested in concrete administrative procedures, where individual privacy comes into direct contact with the needs of state management and the guarantee of social security.

On that basis, this article analyses the legal mechanism for protecting children's personal health data in the implementation of sickness insurance benefits in Vietnam. Its central purpose is not to deny the value of digital transformation or social security policy, but to identify the new regulatory demands that arise when children's health data are incorporated into an intersectoral administrative processing chain. The article argues that protecting children's health data in the sickness insurance regime is not merely a matter of administrative procedure or technical security. It is a legal requirement tied to privacy, dignity, and the best interests of the child. For this requirement to be effectively implemented, legal reform must be accompanied by legal education for families, schools, healthcare facilities, enterprises, and social insurance agencies. Only when each actor in the data life cycle understands the limits of processing and its own confidentiality obligations can social security entitlements be guaranteed without diminishing children's data rights.

2. Literature Review and Theoretical Framework

Identifying the limitations and gaps in the procedure for settling sickness benefits when an employee takes leave to care for a sick child under seven years of age must be situated within the relationship between administrative management, verification of eligibility for social insurance benefits, and the protection of children's

personal data. Under social insurance law, benefit settlement requires the collection, circulation, and processing of information concerning the child's health status through medical records, medical documents, and electronic data. In the context of digital transformation and expanding data interoperability, such information may become accessible to multiple actors involved in the settlement process. The issue, therefore, is not confined to the technical design of forms or administrative procedures. It also concerns the scope of rights and responsibilities of actors authorised to process children's sensitive personal data. From a legal perspective, this is a question of balancing the transparency and efficiency of the social security system with the obligation to respect and protect children's privacy, especially because children do not yet have the full capacity to safeguard their own rights and interests in the digital environment.

In contemporary legal scholarship, the right to privacy has undergone a significant process of reconstruction. It is no longer confined to the nineteenth-century Western classical conception of the "right to be let alone" but is increasingly understood as the right to informational self-determination and control over personal data in a hyperconnected society (Thái, 2012, p. 45). The substantive content of privacy therefore includes each individual's capacity to determine who may collect, retain, use, and share information about them, while also establishing limits on the purposes, scope, and conditions of access to such information (Vũ & Lê, 2020, pp. 55–56). When this theoretical framework is applied to children, the issue becomes more complex. Children are rights-holders, yet they have not fully developed the cognitive, psychological, and legal capacity required to exercise privacy rights

independently. The United Nations Convention on the Rights of the Child affirms that children have the right to protection against arbitrary or unlawful interference with their privacy, family, home, correspondence, honour, and reputation, while the principle of the best interests of the child must serve as the guiding standard in all

decisions concerning children (Nguyễn N. et al., 2025, p. 326).

At the intersection of legal protection and digitalisation, a structural paradox gradually becomes visible. The laws of many countries, including Vietnam, allow parents or guardians to represent children in giving consent to the processing of personal data. This substituted-consent mechanism has a protective basis, yet in certain contexts it may weaken the child's own voice in relation to data about themselves. Children are therefore easily placed in the position of passive data subjects, almost entirely dependent on the awareness, prudence, and digital competence of adults (Phạm & Phan, 2020, p. 18). This is not a simple technical loophole. It is the consequence of a protective mode of thinking formed before personal data acquired the capacity to circulate, be copied, reused, and linked on a large scale as it can today.

Within an ever-expanding data ecosystem, children's health data occupy a special position compared with ordinary administrative identifiers. Such data do not merely reflect a health condition at a particular point in time. They may also contain information that remains attached to an individual's life over the long term, such as congenital medical history, blood type, genetic factors, neuropsychiatric diagnosis, or disability status (Nguyễn G., 2024, p. 74). Once disclosed, much health information cannot be meaningfully retrieved. A person whose password is exposed can change it. A person whose card information is leaked can block the card. But a child whose disease code, clinical diagnosis, or sensitive treatment record has been disclosed may have to face consequences extending far beyond the moment of the incident. The consequences of unauthorised disclosure or leakage of children's health data are not confined to cybersecurity risks. They also threaten the child's right to normal development, the right to be free from stigma, and future opportunities for social inclusion. (Đoàn & Trần, 2025, p. 231). In cases involving developmental disorders, infectious diseases, mental health conditions, or congenital abnormalities, health data that are disseminated

without proper control may become material for cyberbullying, extortion, discrimination, or more subtle forms of social exclusion. Recognising this sensitivity, Vietnam's Law on Personal Data Protection 2025 classifies health information contained in medical records as sensitive personal data, thereby requiring a higher level of protection from data-processing actors (Quốc hội, 2025, Art. 9). Even so, the legal recognition of a concept does not automatically produce substantive protection, especially when such data enter a mandatory, multi-party administrative cycle with multiple transit points outside the medical sector.

It is precisely at the intersection between administrative management and human rights protection that the strain within the current mechanism becomes most visible. The state, as the actor responsible for managing and regulating public welfare funds, has legitimate grounds for establishing appraisal mechanisms to prevent fraud in the enjoyment of sickness insurance benefits. Current insurance law requires an employee who takes leave to care for a sick child under seven years of age to provide valid medical grounds as the basis for benefit settlement (Quốc hội, 2024, Art. 118). This requirement pursues a lawful objective. The issue lies in the degree of data disclosure required and the range of actors permitted to access it. When parents must provide documents containing their child's diagnosis, disease name, or disease code to enterprise human resources staff, accounting personnel, and social insurance officers, the child's health data have already left the professional confidentiality space of the medical treatment relationship. These receiving actors are not directly involved in treatment, have no professional need to know the child's full medical condition, and are not always subject to a confidentiality standard equivalent to medical ethics. Viewed through the lens of data ethics and personal data protection law, this situation raises serious concerns about the principle of data minimisation. Under this principle, the collection and processing of data should be limited to what is sufficient to achieve the lawful purpose of the transaction or procedure (Bùi, 2025, p. 314). If

the purpose pursued by the enterprise and the social insurance agency is to confirm that the child has an illness giving rise to the parent's entitlement to leave and benefits, the necessary question is whether these actors truly need to know the specific disease, ICD code, or clinical description. A more rationally designed mechanism would distinguish between data proving eligibility for the benefit and detailed pathological data. When this boundary is blurred, a social security procedure may inadvertently become a channel for collecting health data beyond the needs of processing. This imbalance does not negate the objective of managing the insurance fund. It shows only that digitalisation and procedural standardisation must be accompanied by privacy impact assessment, rather than assuming that all information appearing in medical documents may be circulated through administrative links.

International experience offers a useful frame of reference for identifying the depth of the problem. In Europe, the General Data Protection Regulation classifies health data as a special category of data and, as a general rule, strictly restricts its processing except in legally permitted circumstances such as preventive medicine, medical diagnosis, the provision of healthcare services, or the management of healthcare systems, provided that such processing is tied to professional secrecy or an equivalent duty of confidentiality (European Union, 2016, Art. 9). In employment relations, this approach encourages the separation of access rights between human resources departments and healthcare professionals. The employer needs to know only that the employee has a valid ground for leave and the necessary duration of absence, not the full medical diagnosis of the employee or the employee's child. According to some comparative analyses, the European model of data governance tends to separate data confirming eligibility for benefits from detailed pathological data, thereby reducing the risk of information leakage by non-medical intermediary actors (Bùi, 2025, p. 315). In the United States, the Health Insurance Portability and Accountability Act establishes a mechanism for protecting

personal health information, under which protected health information may not be arbitrarily transferred to an employer unless legal conditions concerning purpose, authorisation, and scope of use are satisfied.

These experiences reveal an important argument. Ensuring the integrity of the social security system and preventing losses to the insurance fund do not necessarily require expanding the access of non-medical third parties to children's pathological data. The core difference in progressive data governance models lies not only in encryption techniques or prohibitive sanctions. It also lies in a philosophy of purpose-based data governance, role-based access limitation, and a culture of compliance formed through professional legal education. In Vietnam, the habit of sharing information incautiously in the digital environment, an administrative management mindset still heavily dependent on evidentiary paperwork, the complacency of parents, and the inevitable lag of legislative technique behind technological development have together made potential points of health-data leakage capable of accumulating into a systemic problem. For that reason, the theoretical review and comparative international experience do more than help identify shortcomings in the process of issuing and using certificates of leave for social insurance benefits. They also provide the foundation for affirming that institutional reform must proceed together with legal education for each group of actors in the data life cycle. Only when healthcare facilities, enterprises, parents, and social insurance agencies all understand the limits of their data processing can the protection of children's health data move from legal principle into everyday administrative practice.

3. Research Methodology

This article adopts an interdisciplinary approach, combining normative legal analysis, business process analysis, and practical case study. These three methods are not used as discrete operations but are arranged within a unified research sequence. The article first establishes the

legal framework governing children's health data in the procedure for claiming sickness insurance benefits. It then traces the movement of data across the actors involved in dossier processing. Finally, the identified risks are tested against practical incidents and social behaviours that may reduce the effectiveness of data protection.

Normative legal analysis is the central method of this study. The article systematises and analyses the provisions of the Law on Personal Data Protection 2025, Decree No. 356/2025/ND-CP, and other legal instruments relevant to the identification, processing, and protection of sensitive personal data in the health sector and in relation to children (Quốc hội, 2025; Chính phủ, 2025, Art. 3). The focus of this analysis does not stop at describing the content of legal norms. It also evaluates the extent to which those norms can be translated into a concrete administrative procedure. At the same time, the Law on Social Insurance 2024 is approached from the perspective of determining the conditions under which an employee's right to sickness benefits arises when caring for a young child, while also examining the reasonable boundary between the requirement to prove eligibility for benefits and the privacy of children's health data (Quốc hội, 2024). Comparative legal method is incorporated to compare Vietnam's legal framework with certain international standards on health data protection, particularly the European Union's General Data Protection Regulation. This comparison is not intended to impose an external model. Rather, it helps clarify the requirements of data minimisation, purpose limitation, and control over consent given by a legal representative in relation to children's data.

To move legal provisions from the textual plane to the operational plane, the article uses business process analysis to construct a data-flow map. The central object of analysis is Form No. 07, namely the certificate of leave for social insurance benefits prescribed in Circular No. 25/2025/TT-BYT (Bộ Y tế, 2025, Form No. 07). The article follows the circulation of this document from its creation at a medical examination and treatment facility, its transfer to

the parent, its receipt by the enterprise's human resources or accounting department, and its subsequent declaration, digitisation, and processing on platforms within the social insurance system. This approach makes it possible to identify the points at which children's pathological data may be exposed to non-medical actors. On that basis, the study assesses whether the current process satisfies the principle of data minimisation or still tacitly allows multiple actors to access detailed pathological information beyond what the procedure requires.

The practical case-study method is used to test risks

from the perspective of social evidence. Based on information gathered from incidents involving the leakage or unlawful exploitation of electronic medical records reported by the press and professional commentators, the article analyses the risks arising when healthcare personnel or persons with system access use patient data for improper purposes (VietTimes, 2020). At the same time, the study also considers risks arising from parents' habits of sharing information in the digital environment, especially the practice of sending original certificates through messaging applications, internal groups, or communication channels that lack adequate control. These two groups of risks have different origins. One arises from the abuse of access rights. The other stems from gaps in awareness and digital legal literacy. Yet both converge at the same point. They weaken the ability to control children's health data once such data have left the medical treatment space. The combination of these three methods enables the article not only to describe legal provisions but also to examine the compatibility among norms, procedures, and actual behaviour. Normative legal analysis identifies the required standard of protection. Business process analysis shows where that standard is implemented or weakened along the chain. Practical case study explains why data risks cannot be addressed only through post-violation sanctions. On this basis, the article argues that protecting children's health data in the sickness insurance regime should be approached as a

problem of institutional reform linked to multi-actor legal education, rather than merely as a matter of improving forms or strengthening technical security.

4. Research Findings

The research findings reveal a number of limitations in the governance of children's health data when employees carry out procedures for claiming sickness benefits under Vietnam's Law on Social Insurance. During the benefit settlement process, children's health data are not processed solely within medical examination and treatment facilities, but are also transferred to employers and social insurance agencies through electronic systems. Digitalisation has contributed to simplifying procedures, shortening dossier-processing time, and improving administrative efficiency. However, when children's pathological data become accessible to multiple actors, the risk of privacy infringement also increases, particularly where those actors do not perform a medical function or are not subject to confidentiality obligations equivalent to those imposed on medical examination and treatment facilities.

On that basis, this section identifies the principal manifestations of data risk across the entire procedure for implementing sickness insurance benefits. The analysis focuses on the misalignment between the legal framework for personal data protection and sectoral rules on healthcare and social insurance, the points of data leakage that may arise from hospital systems and electronic medical records, the risk of leakage in the enterprise environment when children's health data are treated as an employment-related document, and the practical limits of traditional protection mechanisms such as consent, data control rights, and the right to request erasure in a mandatory social security procedure.

4.1. Legal Misalignment in the Processing of Social Insurance Data

The period from 2024 to 2025 marked an important transition in Vietnam's legal system governing personal data, social security, and digital governance. The Law on Personal Data

Protection 2025 and Decree No. 356/2025/ND-CP established a new legal foundation for the identification, processing, and protection of sensitive personal data. Under this approach, information relating to health status, biometric data, and genetic characteristics is classified as sensitive personal data, requiring a higher level of protection than ordinary identifying data (Chính phủ, 2025, Art. 4). For this category of data, agencies and organisations acting as data controllers or data processors must comply with stricter legal obligations, including the requirement to conduct a personal data processing impact assessment in circumstances prescribed by law (Quốc hội, 2025, Art. 21). When the data subject is a child, the protection requirement must be approached with still greater caution, since children lack the full cognitive, legal, and social capacity to protect their own data against complex processing flows.

This legislative progress, however, encounters a notable bottleneck when measured against sector-specific law on healthcare and social insurance. The Law on Social Insurance 2024 recognises an employee's right to sickness benefits where the employee must take leave to care for a sick child under seven years of age (Quốc hội, 2024, Art. 118). To prove eligibility for the benefit, the employee must submit a certificate of leave for social insurance benefits using the form issued by the competent authority. This document is Form No. 07, promulgated together with Circular No. 25/2025/TT-BYT (Bộ Y tế, 2025, Form No. 07).

The difficulty is that this form does not merely certify the fact that the child is ill and the number of days for which the employee needs leave to provide care. It may also contain detailed medical information, including diagnosis, disease name, disease code under the international classification, or treatment method (Bộ Y tế, 2025, Form No. 07). The same procedural flow therefore places two different legal requirements under tension. Personal data protection law requires restricted access to

sensitive health data. The insurance procedure, by contrast, may require that such information pass through several intermediary actors for the purpose of assessing entitlement to social security benefits. This misalignment becomes clearer when placed within the policy of interoperating medical examination and treatment data, population data, and insurance data under Decision No. 69/QĐ-TTg of the Prime Minister (Thủ tướng Chính phủ, 2025). Data interoperability is a necessary reform direction, helping reduce paperwork, shorten processing time, and strengthen public

governance capacity. Yet procedural reform is compatible with data protection only when the system can distinguish between data necessary to verify eligibility for benefits and detailed pathological data that should be shielded from actors without a medical function. If the system architecture is designed to share the entire content recorded in the certificate, the principle of data minimisation risks being weakened at the design stage itself, even before any individual violation occurs during implementation.

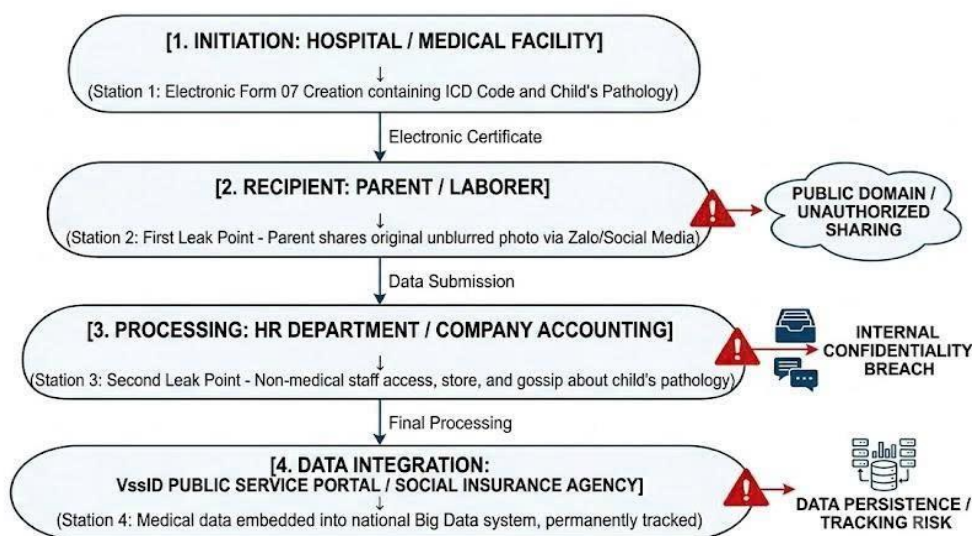


Figure 1. Data Flow Diagram of the transfer of the Sickness Insurance Leave Certificate (Form 07) and sensitive child medical data leak points.

As the data-flow diagram in Figure 1 shows, the movement of Form No. 07 may require a child's medical data to pass through non-medical transit points, most notably the human resources or accounting department of the enterprise where the father or mother works. In this relationship, the enterprise is not a treatment provider, has no professional need to access the child's full medical condition, and is not always subject to a professional confidentiality standard comparable to that imposed on medical examination and treatment facilities. Based on the concept of actors participating in data processing under the Law on Personal Data Protection 2025, these actors may be regarded as recipients or third parties in certain processing situations (Quốc hội, 2025, Art. 2). The possibility that a non-medical actor may access a child's diagnosis,

such as an infectious disease, congenital abnormality, or neuropsychiatric disorder, merely to verify the parent's eligibility for leave and benefits, raises serious concerns about data excess. This is not only a confidentiality risk. It also indicates that the processing purpose and the scope of collected data have not been sufficiently differentiated.

To clarify the level of this risk, the article constructs a matrix comparing the mandatory information fields in Form No. 07 with the personal data protection principles under the Law on Personal Data Protection 2025. This matrix separates each data group according to its processing function, including identifying data, data confirming the illness, detailed pathological data, and data used for benefit payment. This distinction is important because not all data

appearing in a medical certificate are necessary for every actor in the processing chain. The enterprise may need to know that the employee has a valid ground for leave and the corresponding leave period. The social insurance

agency may need information to control payment under the correct regime. But this administrative need does not automatically entail a right to access the child's entire clinical diagnosis.

Table 1. Matrix comparing medical data fields in Form No. 07 under Circular No. 25/2025/TT-BYT with risks of violating the principle of data minimisation

Mandatory information fields required in Form No. 07	Legal classification under Decree No. 356/2025/ND-CP	Assessment of the degree of violation of the principle of “data minimisation” when circulated through the enterprise
1. Patient identification, including full name, date of birth, health insurance card number, and personal identification number of the child	Basic personal data and children's data requiring special protection.	Low level. This information is necessary for the enterprise to identify the person concerned and prove the family relationship between the employee and the child.
2. Diagnosis, including clinical disease name and ICD-10 international disease code	Sensitive personal data, namely information concerning physical and mental health status.	Particularly serious level. The enterprise only needs to know that the “child is ill and requires parental medical care” in order to approve leave benefits. A form-based system that compels the disclosure of the specific disease name or ICD code to human resources staff results in excessive data collection, exposes the child's private life to persons not bound by medical confidentiality, and creates conditions for stigma.
3. Treatment method, including internal medicine, surgery, or interventional procedure	Sensitive personal data, namely medical record information.	Serious level. This creates a risk of judgment or gossip within the workplace concerning the child's health status. This data adds no further evidentiary value for the purpose of disbursing social insurance funds.
4. Recommended leave period, from date to date	Ordinary administrative or accounting data.	Reasonable. This is the only data field that is genuinely necessary and central for the enterprise and the social insurance agency to calculate the benefit amount.

The analysis in Table 1 allows a foundational conclusion to be drawn. The central conflict in the current mechanism does not necessarily lie in a direct contradiction among statutes. It lies instead in the misalignment between an administrative-document management mindset and the data protection standards of contemporary human rights law. Form No. 07, even when digitised and incorporated into electronic declaration platforms, still bears the

imprint of a paper-based administrative era, in which medical information was commonly treated as an assumed component of a dossier proving financial entitlement. When an administrative form has not been refined according to the principles of tiered access, masking of sensitive data, and purpose limitation, system-level cybersecurity barriers may not be sufficient to protect children from the point at which data are generated. In other

words, the risk does not lie only in whether data are attacked or breached. The risk already arises when the procedure requires the collection and circulation of more data than necessary.

4.2. Internal Risks in Electronic Medical Records

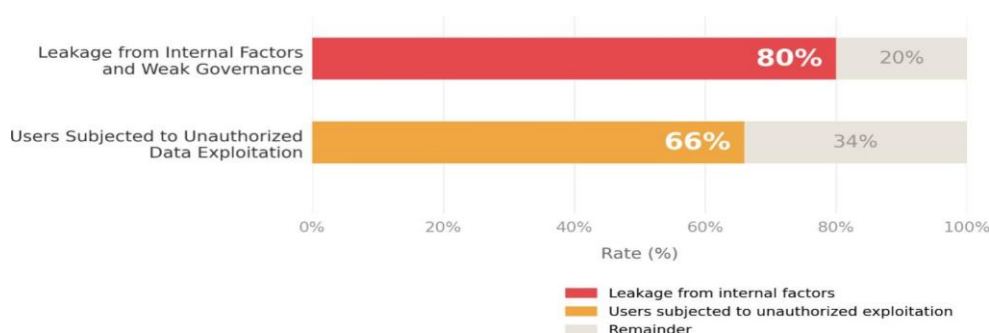
In the procedure for settling sickness benefits under the Law on Social Insurance, medical examination and treatment facilities are the first actors to collect, store, and certify children's health information as the basis for benefit entitlement. At present, alongside digital transformation in the healthcare sector, many healthcare facilities have adopted electronic medical records and medical examination and treatment information management systems in place of traditional storage methods. These systems contain a wide range of children's sensitive personal data, including identifying information, health status, diagnoses, and treatment history. Given the specific nature of health data, the collection and retention of such information serve not only medical examination and treatment activities but also the implementation of procedures for claiming social insurance benefits. Ensuring data security and confidentiality from the very first stage of the process is therefore essential to protecting children's privacy and best interests.

The centralisation of health data brings clear clinical value. Physicians can monitor disease progression, reduce duplicate testing, improve coordination in treatment, and enhance hospital management efficiency. Yet this very centralisation also creates a significant

concentration of risk. When multiple layers of children's information are stored within the same system, any weakness in access authorisation, access monitoring, or internal discipline may expose data on a far larger scale than was possible under paper-based records. The risk therefore does not arise only from external cyberattacks. It may originate inside the healthcare facility itself, where persons with system-access accounts can view, copy, extract, or forward information beyond the scope of their assigned duties.

The practice of hospital data governance shows that access authorisation remains a point requiring particular attention. In a system designed according to the principle of privacy protection from the outset, each individual should be allowed to access only the amount of data necessary for the proper performance of their professional function. The treating physician needs relatively complete clinical data. Administrative staff may need only identifying information and the file code. The hospital-fee accounting department needs data for payment purposes, but not necessarily the entire professional diagnosis. If these boundaries are not clearly established in the software and in internal regulations, staff who are not directly involved in treatment may still be able to view or extract children's medical records. This is the point at which the principle of data minimisation is weakened not because technology is absent, but because access-right design has not been sufficiently aligned with processing functions.

Figure 2. Risk Rates and Causes of Personal Data Leakage in Vietnam's Digital Environment (2021-2024)



In the procedure for issuing the certificate of leave for social insurance benefits under Form No.

07, this risk is further extended. When a parent requests the healthcare facility to issue a certificate

for submission to the enterprise, the child's pathological data are transferred from the treatment space into the space of administrative documentation. The acts of data entry, confirmation, printing, or file export from the hospital management system may leave digital traces connected to the parents' identifying information, long-term stigma.

The data-security figures for Vietnam presented in Figure 2 further clarify the limits of a purely technical approach. When a large proportion of information leaks is attributed to carelessness, intentional misconduct, or weak internal management by users with system access (Thế Lâm, 2021), firewalls, the child's information, diagnosis, and disease code. Once the document is created in the form of a paper copy, photograph, or ordinary PDF file, the technical layer of protection inherent in the hospital system is substantially narrowed. The data are no longer controlled through login mechanisms, access logs, or internal authorisation, but begin to circulate through the hands of different actors.

More significantly, internal risks within healthcare facilities are not merely hypothetical. Several cases reported by the press show that persons with system access have abused their position to collect, copy, or unlawfully transfer patient information to third parties, including data such as age, medical condition, and family contact information (VietTimes, 2020). In paediatrics, this type of data has particular commercial value for businesses dealing in milk products, functional foods, healthcare services, special education, or life insurance. When children's pathological data are commercialised, the harm does not stop at intrusive advertising. Families may be targeted by unverified medical services, scam calls, or forms of exploitation that prey on parental anxiety. Children, where the data relate to infectious diseases, developmental disorders, mental health conditions, or congenital abnormalities, may also face the risk of

security software, or encryption measures can be seen as only one part of the solution. For children's electronic medical records, the most serious risk often does not lie in the system being

attacked from outside. It lies in the fact that insiders are granted access broader than their work requires, yet no adequate post-access control mechanism exists. Without sufficiently detailed access logs, alerts for abnormal retrieval, role-based access control, and clear internal disciplinary rules, detecting the unauthorised copying or transfer of health data will be extremely difficult.

From a legal perspective, the unlawful exploitation or disclosure of children's electronic medical record data may infringe several layers of rights and obligations at once. These include the child's right to privacy, the healthcare facility's duty to maintain patient confidentiality, the obligation to protect sensitive personal data, and the responsibility to ensure information security in the digital environment. The Law on Personal Data Protection 2025 establishes protection requirements for sensitive data and children's data, under which data-processing principles must be observed from collection, storage, and use to sharing and erasure (Quốc hội, 2025, Arts. 9, 24). The greatest challenge, however, does not lie in determining whether a confidentiality obligation exists. It lies in the capacity to prove the violation, identify the path taken by the data after extraction, and quantify harm once the data have spread beyond the original control system. The overlap among medical professional requirements, administrative requirements, and data protection requirements therefore makes the healthcare facility a particularly important link in the entire data life cycle. If a hospital views Form No. 07 merely as a document serving the settlement of insurance benefits, privacy risks will be underestimated at the very point of data generation. Conversely, if this certificate is properly understood as a document containing sensitive health data of children, the procedures for issuance, export, transfer, and logging must be designed with greater caution. Printing a paper copy or issuing an open-format file for parents to submit to the enterprise may be procedurally convenient, but it also substantially reduces the capacity to control data. This is why data protection in the procedure for claiming sickness insurance benefits cannot stop at the

level of declared principles. It must enter each concrete operational act of the healthcare facility, from access authorisation, masking of sensitive information fields, control over file export, and recording of access logs to staff training on legal responsibility when processing paediatric data.

4.3. Children's Health Data in Labour and Insurance Procedures

After leaving the management system of the healthcare facility, children's pathological data enter a processing environment of a different nature, namely the enterprise environment. Under the procedure for implementing social insurance benefits, in order to have sickness allowance considered and settled when taking leave to care for a sick child under seven years of age, the employee must submit the certificate of leave for social insurance benefits to the employer (Quốc hội, 2024, Art. 96). At this transit point, children's health data are no longer confined to the relationship among the medical examination and treatment facility, the patient, and the family. They are incorporated into an administrative processing chain connected to employment, wages, and insurance. Viewed through the lens of the Law on Personal Data Protection 2025, when receiving, retaining, or forwarding Form No. 07, the enterprise may assume the status of an actor participating in the processing of personal data concerning the pathological information of the employee's child (Quốc hội, 2025, Art. 2). Confidentiality obligations should therefore not be understood as a matter of voluntary ethics, but as a legal responsibility attached to the processing of sensitive data concerning a child's health status under Decree No. 356/2025/ND-CP (Chính phủ, 2025, Art. 4). In practice, however, the operation of many enterprises reveals a considerable gap between this legal obligation and their compliance capacity in everyday human resources management.

The first gap arises from the human factor in human resources and accounting departments. Unlike physicians, nurses, or healthcare personnel, who are trained in a professional

environment where patient confidentiality is required, human resources staff mainly perform tasks relating to labour administration, dossiers, wages, and insurance. They have no treatment function, do not need to make medical-professional assessments, and are generally not adequately trained in health data ethics. When the insurance procedure allows them to receive the original Form No. 07, they may see information concerning a child's diagnosis, disease code, or treatment method, although the enterprise's operational need is mainly to determine whether the employee has a valid ground for leave and the corresponding number of days of absence. It is precisely this disparity between the processing need and the scope of data accessed that creates the risk of processing beyond purpose. In the workplace, where personal information can easily circulate through oral exchanges, internal messages, or uncontrolled sharing habits, the pathological data of an employee's child may become the subject of gossip, speculation, or social judgment. For children with sensitive conditions such as developmental disorders, infectious diseases, mental health issues, or congenital abnormalities, such leakage may cause harm far beyond the scope of an ordinary labour procedure.

In addition to the human factor, non-standardised digitisation practices inside enterprises further amplify the risk. In the context of digital transformation in human resources management, it is fairly common for employees to photograph Form No. 07 and send it via Zalo, Viber, personal email, or internal chat groups in order to request leave, confirm a dossier, or transfer supporting documents to the accounting department. These image files are often not redacted to conceal sensitive information, are not subject to controlled retention periods, and may be scattered across the personal devices of multiple individuals. Even when the data are entered into internal human resources or accounting software, the risk is not eliminated if the system has not been designed according to the principle of privacy protection from the outset. A software system that needs only to store supporting documents for benefit

payment purposes but allows multiple employees to access the entire attached dossier at any time weakens the principles of purpose limitation and data minimisation in the spirit of the Law on Personal Data Protection 2025 (Quốc hội, 2025, Art. 9).

The risk chain continues to expand when data are declared to the insurance system through the Public Service Portal and the VssID application. It cannot be denied that the development of VssID and the implementation of high-level online public services constitute an important step in the modernisation of public administration, helping to reduce paperwork, accelerate processing, and improve citizens' ability to monitor their participation in and enjoyment of social insurance (Tạ & Nguyễn, 2022, p. 98). Yet administrative efficiency does not automatically mean data safety. If the electronic procedure still requires enterprise human resources officers to enter, upload, or forward detailed medical information about children, including diagnoses, disease codes, or original attached documents, sensitive data must still transit through the enterprise before reaching the social insurance agency. This transit both creates the risk of data-entry errors and, in practice, reinforces the enterprise's role as a point of retention and processing for children's health data, even though the enterprise is not an actor with a medical function. After being transmitted into the insurance system, children's health data may continue to leave traces in databases serving state management. The interoperability of healthcare, population, and insurance data under Decision No. 69/QĐ-TTg of the Prime Minister is a necessary direction of reform, especially as the state seeks to reduce paperwork and strengthen data-driven governance capacity. Yet data interoperability is genuinely safe only when accompanied by access authorisation mechanisms, access logging, abnormal retrieval monitoring, anonymisation, or pseudonymisation of sensitive data in cases where direct identification is not necessary. If an operational account at the grassroots level can view or extract more than what is needed, the risk no longer lies in the misconduct of a single

individual. It becomes an architectural risk of the entire processing chain. In relation to children's data, this risk must be approached with particular caution because its consequences may not arise only at the moment when sickness benefits are settled. They may extend into the future if health data are retained, linked, or reused beyond the original purpose.

From the perspective of implementing sickness benefits under the Law on Social Insurance, the employer acts as an intermediary responsible for receiving the dossier and transmitting it to the social insurance agency. In this process, the enterprise may access certain information concerning the child's health status that is used as the basis for benefit entitlement. The issue is not the enterprise's participation in the benefit settlement process itself, but the scope within which such data may be accessed, used, retained, and protected. In the absence of internal control procedures and adequate awareness of personal data protection, risks may arise from data leakage or from the use of information beyond the purpose of benefit settlement. Accordingly, alongside the digitalisation of social insurance procedures, it is necessary to strengthen data governance mechanisms and the confidentiality responsibilities of enterprises in order to safeguard children's privacy in.

4.4. Limits on the Enforcement of Data Rights in Health Insurance Procedures

The final gap in this analytical chain is not merely technical or administrative. It touches the very foundation of personal data control in a rule-of-law state. Under the approach of modern data protection law, informational self-determination operates through several core mechanisms, most notably the consent of the data subject, the right to withdraw consent, the right to control the scope of processing, and the right to request erasure or restriction of data processing. The Law on Personal Data Protection 2025 recognises consent as an important legal basis for personal data processing, while emphasising that consent must be voluntary, clear, and consistent with the processing purpose (Quốc hội, 2025, Art. 11). The Law also grants

individuals rights relating to access, provision, correction, erasure, or restriction of the processing of their data under certain conditions (Quốc hội, 2025, Art. 4). These are progressive legal safeguards, especially for children as a group of subjects requiring special protection. Yet when placed within the procedure for payment of sickness benefits, these rights reveal significant limits in implementation.

The first limit lies in the nature of consent within employment and social insurance relations. In formal terms, parents or legal representatives of children may be the actors who provide the child's medical dossier to the enterprise and the social insurance agency. In reality, however, that decision is not made in an entirely free environment. An employee who wishes to have sickness benefits settled when taking leave to care for a child must submit a certificate of leave for social insurance benefits as required by the sectoral procedure (Quốc hội, 2024). When a social security entitlement depends on the provision of a medical document, parents are placed before a narrow choice. They may submit the dossier, which means accepting that their child's pathological data will pass through the enterprise and the social insurance agency. Or they may refuse to submit it, which means risking the denial of an allowance that the law has designed to protect the family at the moment when the child is ill. In that context, consent exists procedurally, but its substantive voluntariness is considerably weakened.

It is important to note that this weakening of voluntariness does not arise from direct coercion by a particular individual or agency. It arises from the structure of the administrative procedure itself. When the process requires a document containing detailed pathological information, while the system has not yet provided a safer alternative such as a confirmation of eligibility separated from the clinical diagnosis, parents have little real capacity to control the scope of data shared. The consent mechanism is therefore transformed into a procedural device that legitimises data circulation rather than serving as a tool for protecting informational self-

determination. In the case of children, the issue is even more sensitive because the subject directly affected by the data is the child, while the decision-maker is the parent or representative. The gap between the person who decides and the person who bears the consequences makes substituted consent a mechanism that requires stricter supervision in social security procedures involving health data.

The second limit lies in the right to withdraw consent and the right to request data erasure. In legal terms, these rights create a mechanism through which individuals are not permanently bound by a past decision to share data (Quốc hội, 2025, Art. 4). In the social insurance process, however, data are not processed merely to complete a single transaction. After Form No. 07 has been submitted to the enterprise, received, digitised, and transferred into the insurance system, the data may be retained for various governance purposes, including verification of benefit eligibility, comparison against payment history, inspection, auditing, and fraud prevention. These are all management purposes with certain legal grounds. Yet this multiplicity of purposes makes the right to request erasure difficult to implement in practice, especially where the system has not clearly separated the data that must be retained to evidence a financial transaction from the detailed pathological data that may be masked, pseudonymised, or access-limited after payment has been completed.

A core legal issue therefore emerges. The social insurance system has a legitimate need to preserve the integrity of payment records. But that need does not necessarily require the long-term retention of all detailed pathological information concerning children in a directly identifiable form. If diagnostic data, disease codes, or treatment information continue to exist in enterprise records and insurance systems without mechanisms for access authorisation, anonymisation, pseudonymisation, or time-bound access limitation, the data subject's right to erasure will have only limited value. In other words, the problem does not lie in whether the law

recognises the right. It lies in whether the operational system is designed to allow that right to function.

To highlight this mismatch, the article establishes the comparative matrix in Table 2 between the rights of data subjects under the Law on Personal Data Protection 2025 and the way those rights are implemented in the social

insurance process. The matrix shows an important reality. The rights to consent, withdraw consent, control processing purposes, and request data erasure all have protective significance at the normative level. Yet once they enter a mandatory social security procedure tied to medical documentation and payment records, those rights are easily limited by the operating structure of the system itself.

Table 2. Comparative matrix of the conflict between data subject rights under the Law on Personal Data Protection 2025 and the practice of social insurance procedures

Rights of the data subject under the Law on Personal Data Protection 2025	Implementation practice in the procedure for settling sickness benefits under the Law on Social Insurance 2024	Assessment of the level of conflict and risks to children
Right to voluntary consent under Article 11, according to which consent must not be accompanied by coercive conditions.	Parents are effectively compelled to submit Form No. 07 containing detailed pathological information about the child to the enterprise as a precondition for disbursement of sickness benefits.	High conflict. Consent loses its voluntary character, turning children’s health data into a means through which parents must trade privacy for financial entitlement, thereby violating the principle of privacy protection.
Right to withdraw consent under Articles 4 and 10, according to which the subject has the right to withdraw permission for data processing at any time.	Once the dossier has been approved on VssID, the enterprise and the insurance agency must retain supporting documents for inspection and auditing. Parents cannot meaningfully “withdraw” consent.	Practically infeasible. High risk arises once the data have escaped family control and are scattered across third-party accounting software systems.
Right to request data erasure, or the right to erasure, under Article 4, namely the right to request deletion of personal data when the data are no longer necessary.	The national insurance database, or Big Data system, requires permanent log-audit retention of benefit history. There is no mechanism for partial deletion of medical record data from payment dossiers.	Systemic conflict. The child’s right to be forgotten is neutralised. Digital traces concerning sensitive congenital, developmental, or neuropsychiatric conditions may persist indefinitely, threatening the child’s future.

The analysis in Table 2 shows that the core conflict is not the denial of data subject rights in legal texts. It is the lack of compatibility between recognised rights and the technical and operational conditions required to implement them. The current system tends to prioritise the completeness, continuity, and verifiability of insurance dossiers. This priority is necessary for the governance of social security funds. But without supporting protective tools such as

anonymisation, pseudonymisation, masking of sensitive data fields, role-based access authorisation, and differentiated retention periods for each category of data, that priority may undermine children’s privacy. Information such as developmental disorders, congenital disabilities, infectious diseases, or mental health conditions may have long-term effects on a child’s social life. When such information is retained and reused beyond what is necessary, the risk is not

only a present data risk. It is also an accumulated risk to the future of the data subject.

From the limits of these two mechanisms, an important conclusion may be drawn for reform. Protecting children's health data in social insurance procedures cannot rely solely on parental consent or the right to request erasure after the data have already circulated through multiple actors. These rights must still be respected, but they need to be supported by institutional and technical design capable of minimising data from the outset. Legal education for actors involved in data processing is also indispensable. Parents need to understand the limits of sharing their children's data. Enterprises must recognise that Form No. 07 is not an ordinary labour document but a record containing sensitive health data. Healthcare facilities and social insurance agencies need to shift from a mindset of full collection to one of sufficient processing. Only when legal rights are connected to procedural design and a culture of compliance can they operate as instruments of substantive protection rather than remain promises in legal texts.

5. Discussion: Directions for Legal Education on the Protection of Children's Health Data in the Sickness Insurance Regime

The analysis above reveals a notable paradox in the circulation of children's health data within the sickness insurance regime. Healthcare digitalisation, electronic medical records, and interoperable platforms such as VssID are designed to improve governance efficiency, reduce paperwork, and increase transparency in the settlement of social security entitlements. Yet when children's health data are introduced into multiple layers of processing without a sufficiently clear mechanism for tiered access, the very process of procedural modernisation may expand the leakage of sensitive data. In other words, the risk does not lie in technology itself, but in the way technology is embedded in administrative procedures that were not designed from the outset with data protection in mind. The misalignment between the Law on Personal

Data Protection 2025 and sectoral regulations on social insurance, healthcare, and labour therefore reveals an important reality. A progressive legal corridor is a necessary condition, but it is not sufficient to protect privacy if implementing actors do not properly understand the limits of data processing in each operational act.

From a legal perspective, the Law on Personal Data Protection 2025 and Decree No. 356/2025/ND-CP have established a number of new standards for personal data processing, including requirements to prevent default consent, manipulated consent, or the use of misleading instructions in the process of data collection (Chính phủ, 2025, Art. 6). However, the data-leakage points analysed above do not arise only from technical defects, encryption algorithms, or external cyberattacks. They also stem from gaps in awareness and compliance discipline among human actors throughout the entire data life cycle. Healthcare personnel may treat access to medical records as an ordinary internal operation. Enterprise human resources officers may regard Form No. 07 as a labour-related document, rather than as a record containing sensitive health data of a child. Parents may send photographs of certificates through messaging applications without redacting their child's pathological information. When the human factor becomes the vulnerable link in the confidentiality chain, technical measures and ex post sanctions have only limited effect unless they are accompanied by a corresponding foundation of legal awareness.

The issue becomes more complicated in the context of social security relations, which always contain a certain asymmetry between the employee and the system responsible for settling entitlements. The employee must submit a dossier to receive an allowance when the child is ill. The enterprise needs supporting documents to confirm the basis for leave. The insurance agency needs data to verify payment conditions. Within that chain of relations, parental consent to the provision of children's health data may easily be narrowed into a procedural choice rather than a substantive exercise of informational self-

determination. Without technical and operational options that separate data confirming eligibility for benefits from detailed pathological data, consent can hardly achieve its full protective meaning under the spirit of personal data protection law (Quốc hội, 2025, Art. 9). Data rights therefore acquire real value only when data subjects and their representatives have sufficient capacity to recognise risks, while the actors holding processing power are responsible for limiting the scope of collection, access, and retention.

It is from this point that we argue that data governance in the field of social security must move from a purely administrative compliance mindset toward the development of a data protection culture through focused legal education. Legal education in this context is not merely the dissemination of new regulations or the organisation of formal training sessions. It must be understood as an instrument for shaping behaviour, enabling legal principles such as data minimisation, purpose limitation, role-based confidentiality, and the best interests of the child to permeate the everyday operations of hospitals, enterprises, families, and insurance agencies. This approach also avoids placing the entire burden of self-protection on parents, who are in a weaker position in terms of information, procedure, and the need to secure social security benefits.

On that basis, the proposed system of legal education solutions should focus on the links that determine the actual level of data safety in practice. For healthcare facilities, the emphasis should be on translating traditional medical ethics into data ethics, so that physicians, administrative personnel, and hospital governance units understand that electronic medical records are not only professional documents but also sensitive data structures that must be controlled according to access rights. For enterprises and social insurance agencies, mandatory compliance training should be established on the principle of data minimisation, the handling of documents containing health data, and the limitation of dossier retention after the processing purpose

has been fulfilled. For parents, legal education must aim to strengthen their capacity to protect children's digital privacy, especially by developing habits such as redacting pathological information, limiting the transmission of medical documents through group chats, and recognising risks arising from uncontrolled data sharing. In relation to children's data in particular, current law already requires a higher level of protection, including, in certain cases, the need to take into account the consent of the legal representative and of the child when the statutory conditions are satisfied (Quốc hội, 2025, Art. 24). The combination of these three educational axes can create a soft but durable layer of protection, supplementing technical safeguards and legal sanctions in the era of digitalised social security.

5.1. Data Ethics Education for Healthcare Personnel

In the medical tradition, the duty to keep patient information confidential has always been one of the core foundations of medical ethics. However, as the healthcare system enters the stage of digitalisation, together with electronic medical records, hospital information systems, and interoperable insurance-data platforms, confidentiality is no longer tied only to professional admonition or to the safeguarding of a paper file within the hospital. Health data can now be exported, copied, forwarded, stored, and connected with multiple other systems through a single operational act. In this context, traditional medical ethics must be expanded into data ethics, understood as a normative framework that enables healthcare personnel to recognise fully that every act of access, data entry, printing, file transmission, or document confirmation is a form of data processing with legal consequences for the patient's privacy, especially where children are concerned.

The gaps analysed in the preceding section show that risk does not always originate from external cyberattacks. A substantial part of the risk may arise from gaps in awareness among internal personnel themselves. Physicians, nurses, technicians, administrative staff, or

hospital system administrators may still approach medical record data as operational material within the scope of internal management, without fully recognising that such data constitute sensitive personal data directly linked to the personal rights of patients. Where the data concern children, the required level of caution must be higher, since the disclosure of information about infectious diseases, developmental disorders, mental health, congenital disabilities, or special treatment status may produce long-term social consequences.

Acts such as sending patient information through insecure messaging platforms, sharing records in internal groups without a professional need, or abusing access rights to extract lists of paediatric patients for third parties all show that medical ethics, if understood only as a general moral commitment, is insufficient to control data risks in the digital environment (VietTimes, 2020). For that reason, the first direction for legal education should be implemented directly within medical and pharmaceutical training institutions. Personal data protection law, data ethics, and health information security should be integrated into the curriculum as compulsory content, alongside medical ethics. Medical students need early leakage to concrete scenarios involving medical record leaks, abuse of access rights, sharing of images of medical documents, and the processing of children's data. This mode of training helps learners understand that protecting health data is not the separate responsibility of the information technology department, but a fundamental professional competence of medical practice. A physician in the digital era does not only need to examine correctly and treat correctly. They must also know what information may be recorded, what information needs to be shielded, who is entitled to access it, and where the patient's data will go after leaving the consultation room.

For those already working in healthcare facilities, data ethics education should be organised as periodic compliance training linked to real

situations and specific professional responsibilities. Hospitals should not stop at issuing confidentiality regulations or requiring employees to sign general commitments. Training content needs to analyse documented data-leakage incidents and identify the legal, professional, and social consequences for patients. In this regard, it is necessary to emphasise that health-status data fall within the category of sensitive data, while children's data are subject to a higher protection regime under the Law on Personal Data Protection 2025 (Quốc hội, 2025, Art. 24). When healthcare personnel clearly understand that a seemingly minor act, such as taking a screenshot of a medical record, sending a file through a personal account, or opening a record unrelated to the treatment case, may create serious legal risks, the protection mechanism begins to form from within the organisation.

Another important element is to establish the role of the unit or officer responsible for personal data protection within the hospital. This actor should not merely review compliance documents on paper, but should become the core agent for training, supervision, and the diffusion of a confidentiality culture throughout the healthcare facility. Through guidance from the specialised unit, healthcare personnel can learn how to apply the principle of privacy protection from the design stage to everyday operations. These operations include role-based access authorisation, logging out of software after examination shifts, avoiding the use of shared accounts, not transferring medical records through personal devices, refusing unauthorised requests for information, and promptly reporting abnormal access. These requirements may appear small, but they determine whether legal principles enter practice or remain only in written regulations.

Data ethics should also be concretised in the procedure for issuing the certificate of leave for social insurance benefits under Form No. 07. In practice, healthcare facilities must still meet the requirement of certifying illness so that employees can exercise their right to benefits. Yet satisfying an administrative requirement does not

mean recording and transferring more information than necessary. Viewed through the principle of data minimisation, medical practitioners should be guided on how to record diagnoses and certify medical conditions in a manner that provides sufficient professional grounds while limiting the leakage of excessively sensitive details to actors without a medical function. This is particularly important for conditions that may cause social stigma or affect children's opportunities for future inclusion. Caution in every diagnostic line, every disease code recorded, and every file exported is a concrete expression of professional responsibility in the digital environment.

From the perspective of hospital governance, translating medical ethics into data ethics does not mean rejecting the traditional values of the medical profession. It means adapting those values to new technological conditions. When electronic medical record data can leave the hospital faster, travel farther, and be reused for longer periods, the duty of confidentiality must also be understood more broadly, more deeply, and with greater technical specificity. Protecting children in this context is not only a matter of treating their illnesses. It also means protecting them from the social consequences that may arise when pathological data are disclosed beyond what is necessary. Legal education in data ethics for healthcare personnel should therefore be regarded as the first protective layer of the entire social security chain, beginning at the point where data are created.

5.2. Legal Training on the Protection of Children's Health Data in the Sickness Insurance Process

After healthcare facilities, enterprises and social insurance agencies are the two links that play a decisive role in determining the safety of children's health data in the procedure for claiming sickness benefits. When an employee submits Form No. 07 as the basis for benefit settlement, the enterprise is not merely receiving an ordinary employment document. It is accessing a record containing sensitive personal data concerning the employee's child. Viewed

through the lens of the Law on Personal Data Protection 2025, depending on its specific role in each act of receiving, retaining, digitising, or forwarding the dossier, the enterprise may acquire the status of an actor participating in the processing of personal data (Quốc hội, 2025, Art. 2). Similarly, when the social insurance agency receives the dossier through the electronic system for benefit settlement, it must ensure corresponding obligations, including the requirement to conduct a personal data processing impact assessment for sensitive data processing activities where the statutory conditions are met (Quốc hội, 2025, Art. 21). These obligations, however, can hardly enter practice if the persons directly handling the data, especially human resources officers, accounting staff, and insurance officers, have not been adequately trained in privacy rights and the principle of data minimisation.

The central objective of compliance training for human resources officers is to change the way Form No. 07 is perceived. This document should not be handled as an accounting voucher or an ordinary leave application, since it may contain diagnoses, disease codes, treatment methods, and other health data concerning children. Human resources staff do not perform a medical function, do not participate in treatment, and do not need to make professional medical assessments of the child's condition. The enterprise's lawful need lies mainly in determining whether the employee has a valid basis for leave, how long the leave period is, and whether the dossier satisfies the conditions for transfer to the insurance procedure under the Law on Social Insurance 2024 (Quốc hội, 2024, Art. 96). Compliance training must therefore help human resources officers distinguish between data necessary for labour and insurance purposes and detailed pathological data unnecessary for the enterprise's function. Only when this distinction becomes part of professional awareness can the principle of "need to know" acquire the conditions required for actual implementation.

At the operational level, enterprises should be guided to build dossier-handling procedures that

reduce data from the moment of receipt. When receiving Form No. 07, the human resources department should have a process for masking or limiting the display of detailed pathological information before storing the document in the human resources management system, where such fields are not necessary for the purpose of confirming entitlement. Electronic dossiers should be subject to role-based access control, with access limited to persons directly responsible for processing them, and retention periods should be tied to specific processing purposes. Copying the entire original document and storing it in a shared folder, sending it through group chats, or forwarding it through personal accounts must be recognised as conduct that increases data risk, rather than as a normal administrative habit. This is where legal education must reach the level of concrete operational acts, because data risks often do not arise from one major decision but from many small habits repeated every day.

Compliance training must also aim to reshape the culture of digital communication in the workplace. Studies on information security show that human error and non-technical attacks are important causes in many incidents involving personal data breaches and leaks (Đoàn & Trần, 2025, p. 234). In that context, the practice whereby employees or human resources officers photograph the original certificate of leave for social insurance benefits and send it through Zalo, Viber, Telegram, personal email, or internal chat groups can no longer be treated as a harmless convenience. Training programmes must make clear that images containing unredacted health data, once placed on communication platforms outside the enterprise's controlled system, may create legal risks for the sender, the recipient, and the employing organisation. In the event of a violation of personal data protection rules, the organisation may face administrative sanctions under Decree No. 356/2025/ND-CP (Chính phủ, 2025). This awareness provides the basis for enterprises to develop a data-confidentiality code of conduct, in which the circulation of medical records or health documents containing

sensitive data through uncontrolled channels is clearly restricted.

For social insurance agencies, compliance training must be situated within the broader context of public data governance. The implementation of interoperability among healthcare, population, and insurance data under Decision No. 69/QĐ-TTg significantly increases the capacity to process, cross-check, and control social security entitlements. This is a valuable step in the modernisation of state management. Yet when social insurance agencies become the place where large volumes of data relating to health status, benefit history, and citizens' identifying information are received and processed, data protection must be placed on the same level as procedural convenience. Dossier-receiving officers, professional processing officers, and system administrators need regular training on access authorisation, access-history control, detection of abnormal retrieval, processing of children's sensitive data, and the principle of zero trust in information security. Privileged access to a system cannot be understood as a right to use data according to personal discretion. It must always be limited by public-duty purposes, assigned functions, and accountability.

To maintain the continuity of this educational strategy, the role of the unit or personnel responsible for personal data protection in enterprises and state agencies needs to be more clearly established. In accordance with the orientation of Decree No. 356/2025/ND-CP, the actor responsible for personal data protection should not only review procedural compliance, but should also participate in building procedures, updating risk scenarios, organising internal training, and monitoring compliance in practice (Chính phủ, 2025, Art. 35). In small and medium-sized enterprises in particular, where legal and information technology capacity remains limited, this role may be organised flexibly through a specially trained concurrent officer or through external advisory services. What matters is that there must be a responsible focal point for data, rather than allowing sensitive health records to drift freely

among human resources, accounting, legal, and direct management units.

Ultimately, a successful digitalised social security system should not be assessed only by the speed of dossier receipt or the capacity for centralised data storage. A more important measure is whether those who operate the system understand the limits of the data they hold. When human resources officers and insurance officers internalise the principle of data minimisation as a professional reflex, the distance between legal norms and actual behaviour can begin to narrow. At that point, the sickness insurance procedure can still achieve its social security objective without requiring children to pay the price of unnecessary leakage of their health data within the employment environment and public governance system.

5.3. Enhancing Parents' Legal Awareness of Children's Digital Privacy

If physicians, hospital personnel, human resources officers, and insurance officers are the actors involved in data processing within institutional spaces, parents play a decisive role within the family space. Parents are usually the persons who directly receive the certificate from the hospital, transfer the dossier to the enterprise, communicate with the human resources department, and choose how the document is sent in practice. Under civil law and the law on children, parents have rights and obligations to represent their minor children in many decisions concerning health, property, and personal rights. In the digital environment, however, this representative role may become a source of risk if parents lack knowledge of personal data, fail to recognise the sensitivity of health information, or are accustomed to sharing their children's documents as part of everyday communication. Legal education for parents should therefore be regarded as an independent pillar in the strategy for protecting children's health data.

The first objective of parental education is to change awareness of the practice of sharing children's data in the digital environment, often referred to as sharenting. This is the phenomenon

whereby parents post or forward images, information, and stories concerning their children on social networks or messaging platforms. The problem does not lie in every act of sharing about one's child, but in the possibility that parents may inadvertently place in the digital space data sufficient to identify, classify, or evaluate the child in the future. In the procedure for claiming sickness benefits, this risk appears in a very concrete form. After receiving Form No. 07 from the hospital, many parents may photograph the original certificate, revealing the child's full name, date of birth, identifying information, diagnosis, disease code, and treatment period, and then send it through company chat groups, classroom groups, personal accounts, or social media in order to prove the reason for absence from work, seek understanding, or request support. Such conduct usually does not arise from malicious intent. It reflects a gap in awareness that children's health data are not family information that may be freely shared at will, but sensitive personal data requiring a higher level of protection.

Studies on digital behaviour show that users often trade sensitive personal data for immediate utility, convenience, or social interaction without fully considering long-term consequences (Nguyễn Đ., 2021, p. 1767). In relation to children's health data, those consequences deserve particular attention. An image of a certificate containing information about an infectious disease, congenital abnormality, developmental disorder, or mental health condition may be stored, captured, forwarded, or reused beyond the family's intention. Once data have left the parent's device and entered digital platforms, the capacity for actual control declines very quickly. The Law on Personal Data Protection 2025 classifies health status as sensitive data requiring strict protection (Quốc hội, 2025, Art. 9). Posting or sending a child's medical document without shielding necessary information may therefore increase the risk of stigma, mockery, discrimination, or targeting by improper commercial services. In this context, legal education must help parents understand that protecting their child's health data

is not excessive caution, but part of the obligation to protect the best interests of the child.

Alongside awareness change, legal education should equip parents with practical skills to protect data in specific administrative situations. When required to submit Form No. 07 to the enterprise, parents are often in a weaker position in terms of information and procedure, and may therefore readily accept sending the entire original or an unredacted photograph without questioning the scope of data needed. Programmes for legal dissemination and education should accordingly guide citizens on the principle of data minimisation. Before sending a copy of the certificate by email, messaging application, or the enterprise's internal system, parents should be instructed on how to redact information fields that are excessively sensitive if those fields are not necessary for confirming the period of leave, such as detailed diagnosis, ICD code, or treatment method. Redaction must be carried out carefully, without distorting the necessary content of the document and without obstructing the lawful verification rights of the enterprise or the social insurance agency. The aim of this skill is not to oppose administrative procedures, but to help parents complete them within reasonable data protection limits.

Legal knowledge also gives parents a basis for communicating with enterprises when requests arise for data beyond the needs of processing. The Law on Personal Data Protection 2025 recognises the requirement of consent in personal data processing, under which consent must be connected to a specific purpose and must not be turned into a coercive condition beyond what is necessary (Quốc hội, 2025, Art. 11). In that spirit, parents should be encouraged to ask the enterprise which information fields are needed, how long the data will be stored, who may access them, and whether the enterprise can receive a version with pathological information redacted. Such questions should not be understood as obstructing the insurance procedure, but as an expression of legal awareness in protecting

children's data rights. When parents are capable of communicating on a legal basis, they become less passive before administrative requests and are better able to participate in limiting risk at the very point of data transfer.

Another important dimension is the development of a culture of dialogue about privacy within the family. The Law on Personal Data Protection 2025 establishes a special protection mechanism for children's data, under which the processing of data in certain cases must take into account the consent of the legal representative and of the child themselves once the child reaches the statutory age threshold of seven years or older (Quốc hội, 2025, Art. 24). For this provision to enter social life, parents need guidance on how to explain to children, in an age-appropriate manner, that medical records, images of documents, disease names, or treatment information are private data that should not be casually shared with strangers or posted online. Respecting the child's voice in decisions concerning personal data not only satisfies legal requirements but also helps children develop digital citizenship capacities from an early age. A child who knows to ask why their image is being posted, why their document is being sent, and who will see that information is already becoming a subject gradually learning how to protect themselves in a digital society.

From a policy perspective, parental education should be implemented through forms that are more accessible and closer to everyday life than traditional legal dissemination programmes. Healthcare facilities may issue a brief guidance note together with Form No. 07, reminding parents not to send photographs of medical documents through public chat groups and recommending the redaction of sensitive fields before transmitting the document. Social insurance agencies may integrate privacy warnings into VssID or the Public Service Portal when citizens upload dossiers. Schools, parent associations, and social organisations may incorporate children's data protection into digital skills education activities. These small but well-targeted interventions may produce

behavioural change more effectively than general messages about cybersecurity.

In sum, the protection of children's health data cannot rely solely on hospitals, enterprises, or state agencies. Since parents are the persons who directly hold, photograph, send, and explain their children's medical documents, they must be equipped with legal capacity corresponding to their representative role. A modern technical system can still be weakened by a single image of a certificate sent to the wrong place, in the wrong way, or without the necessary redaction. Legal awareness education for parents is therefore not a marginal supporting measure, but a critical closing point in the chain of protection for children's health data in social insurance procedures.

5.4. Institutional and Technical Improvement for the Protection of Children's Health Data in the Sickness Insurance Regime

Legal education can raise awareness and change the behaviour of actors involved in data processing. Yet legal education can hardly achieve its full effect if administrative forms and technological architecture remain designed according to the logic of broad collection, broad sharing, and broad retention. Alongside human training, institutional and technical reform is therefore needed in order to embed the principle of privacy by design into the entire process through which health data circulate within the social insurance system. The focus of this reform is not to weaken the capacity to control payments or prevent fraud against the insurance fund, but to redesign data flows so that each actor can access only the information genuinely necessary for the performance of their function.

First, existing medical administrative forms need to be reviewed and revised, especially Form No. 07 prescribed in Circular No. 25/2025/TT-BYT (Bộ Y tế, 2025). As the analysis above has shown, the use of a single standardised form, in which information on diagnosis, treatment method, and ICD-10 code may appear on the same document that parents must submit to the enterprise, is an important cause of increased

leakage of sensitive data. A more appropriate solution would be to design a tiered form mechanism or role-based modular form. Under this mechanism, the electronic medical record system at the healthcare facility could generate two different versions of the certificate. The medical-professional version would contain full information on diagnosis, disease code, and professional grounds, and would be transmitted directly through a secure channel to the assessment or professional processing system of the social insurance agency. The human-resources administrative version, issued to the employee for submission to the enterprise, would display only minimal information such as confirmation that the child is ill and requires care, the valid leave period, the healthcare facility issuing the certificate, and the identifying information necessary for dossier verification. This design would substantially reduce the access of enterprise human resources departments to detailed pathological data while still preserving the basis for verifying entitlement to benefits.

Second, the information technology infrastructure of public service platforms, including VssID and the social insurance database, needs to be upgraded with security and purpose limitation as central design principles. Decision No. 69/QĐ-TTg of the Prime Minister on electronic interoperability of medical examination and treatment data, population data, and civil status data for the settlement of sickness and maternity benefits creates an important step forward in reducing paperwork and improving dossier-processing efficiency (Thủ tướng Chính phủ, 2025). However, as data interoperability increases the connectivity among systems, the requirements for access control and shielding of sensitive data must also be raised accordingly. Platforms serving enterprises should be configured to automatically extract the payment-eligibility status, number of leave days, and necessary identifying information from the QR code or verification code on the certificate, rather than requiring human resources officers to manually enter or read the child's entire diagnosis. For the social insurance agency's storage system, children's health data should be

separated from ordinary identifying data through techniques such as pseudonymisation, encryption, and role-based access control. When ordinary professional officers process dossiers, the system should prioritise the display of necessary operational status rather than automatically displaying the full pathological content, except where there is clear authority and an explicit professional basis.

Third, all organisations participating in the data-processing cycle, from healthcare facilities and enterprises to social insurance agencies, must seriously implement the obligation to conduct personal data processing impact assessments under the Law on Personal Data Protection 2025 (Quốc hội, 2025, Art. 21). An impact assessment dossier should not be reduced to an administrative document prepared merely to complete a compliance requirement. It should be used as a substantive risk-governance tool, requiring actors to map data flows, identify which data are collected, who may access them, where they are stored, how long they are retained, to whom they are shared, and what corresponding protective measures are applied. For Form No. 07 and documents relating to children, impact assessment should pay particular attention to the transfer points from hospital to parent, from parent to enterprise, and from enterprise to social insurance agency. These are the points at which loss of data control is most likely to occur, yet they are often treated as ordinary administrative operations. Fourth, institutional reform must be accompanied by a clear accountability mechanism among actors in the interoperability chain. Healthcare facilities must be responsible for the accuracy, security, and necessity of the data generated in the certificate. Enterprises must be responsible for the receipt, retention, redaction, access authorisation, and deletion of data after the processing purpose has been fulfilled. Social insurance agencies must be responsible for the receiving infrastructure, access control, logging, and limitation of the display of sensitive data. If these responsibilities are not clearly allocated, data risks will easily be shifted from one actor to another, while children and their families

become the parties who ultimately bear the consequences. The interoperability process should therefore be designed not only to make data move faster, but also to determine precisely who is accountable at each point through which the data pass.

The combination of legal education, form reform, technological upgrading, and data impact assessment can create a multilayered defence model for children's health data. Legal education changes human awareness and behaviour. Form reform reduces excessive data from the outset. Privacy-preserving technology controls access rights and shields data during interoperability. Impact assessment dossiers maintain a regular review mechanism for newly emerging risks. When these protective layers operate simultaneously, the social insurance system can continue to pursue transparency, efficiency, and fraud prevention without forcing children to trade their medical privacy for their family's legitimate access to social security benefits.

6. Conclusion

Digital transformation and data interoperability in Vietnam's social security system are generating significant advances in administrative reform, reducing paperwork burdens and improving the efficiency with which citizens' entitlements are settled. This study, however, shows that one issue requires more careful recognition. Macro-level governance efficiency should not be pursued by unnecessarily expanding access to children's sensitive health data. In the procedure for claiming sickness insurance benefits, the use of Form No. 07 in its current structure may cause information such as clinical diagnosis, ICD-10 disease code, or the child's treatment status to pass through non-medical actors, including human resources staff, enterprise accountants, and insurance officers. This is a sensitive intersection among the objective of ensuring social security, the need to control the insurance fund, and the obligation to protect the privacy of children as data subjects who do not yet possess the full capacity to protect themselves.

From a legal perspective, the issue is not the denial of the need to verify eligibility for benefits. The state, enterprises, and social insurance agencies all have legitimate reasons to ensure that payments are made to the right persons, under the right conditions, and in a manner that prevents fraud. The issue lies in the limits of the data that must be collected, shared, and retained in order to achieve that objective. If an enterprise only needs to confirm that the employee has a valid ground for leave and the corresponding number of leave days, then access to the child's full pathological diagnosis should be reconsidered in light of the principles of data minimisation, purpose limitation, and the best interests of the child. The study therefore affirms that protecting children's health data in the sickness insurance regime is not merely a technical requirement of information security, but a legal requirement tied to privacy, dignity, and the child's long-term development. To address this paradox, interventions must go beyond the strengthening of sanctions or the upgrading of technical firewalls. This article argues that the fundamental solution must combine institutional reform, redesign of technological processes, and focused legal education. Institutionally, Form No. 07 and data interoperability procedures should be reviewed with a view to tiered access rights and, where possible, the separation of data confirming eligibility for benefits from detailed pathological data. Technically, platforms such as VssID and insurance data systems should be designed

according to the principle of privacy by design, prioritising the masking of sensitive data fields, role-based access authorisation, operation logging, and the application of appropriate pseudonymisation or encryption techniques. At the human level, legal education should target each group of actors in the data life cycle, including healthcare facilities, enterprises, insurance agencies, parents, and children who are capable of participating in decisions concerning their own personal data. On the basis of these findings, future research may develop in three directions. The first is to quantitatively assess the psychological and social impacts, as well as the risk of stigma, faced by children when health data are disclosed or used beyond the original purpose. The second is to examine the applicability of artificial intelligence and privacy-enhancing technologies to automatically redact, pseudonymise, or limit the display of sensitive data on public service platforms. The third is to extend the analytical framework to other social security procedures involving flows of sensitive health data, such as maternity benefits, occupational accidents, occupational diseases, or disability allowances. A genuinely progressive digital government system should not be measured only by the speed of dossier processing or the degree of data interoperability. It should also be measured by its capacity to establish humane limits that protect the most fragile digital traces of children in modern administrative life.

References

- Bộ Y tế [Ministry of Health, Vietnam]. (2025). Thông tư số 25/2025/TT-BYT ngày 30 tháng 6 năm 2025 quy định chi tiết thi hành Luật Bảo hiểm xã hội và Luật An toàn, vệ sinh lao động thuộc lĩnh vực y tế [Circular No. 25/2025/TT-BYT dated June 30, 2025, detailing the implementation of the Law on Social Insurance and the Law on Occupational Safety and Health in the healthcare sector].
- Bùi, T. Á. L. (2025). Pháp luật một số quốc gia về bảo vệ dữ liệu cá nhân: Một số bài học kinh nghiệm và giải pháp hoàn thiện pháp luật Việt Nam [Legislation of selected countries on personal data protection: Lessons learned and recommendations for improving Vietnamese law]. *Tạp chí Giáo dục & Xã hội* [Journal of Education and Society], (Kì 1, tháng 4), 314–325.
- Chính phủ [Government of Vietnam]. (2025). Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân [Decree No. 356/2025/NĐ-CP dated December 31, 2025, detailing certain articles and implementation measures of the Law on Personal Data Protection].
- Đoàn, M. H., & Trần, T. T. (2025). Bảo vệ dữ liệu cá nhân tại Việt Nam: Thực trạng và giải pháp [Personal data protection in Vietnam: Current situation and solutions]. *Tạp chí Giáo dục & Xã hội* [Journal of Education and Society].

- Society], (Kì 2, tháng 5), 231–236.
- Duy Anh. (2024). Dữ liệu cá nhân của hơn 66% người dùng Internet bị sử dụng trái phép trong năm 2024 [Personal data of more than 66% of Internet users in Vietnam was unlawfully exploited in 2024]. Tạp chí Luật sư Việt Nam [Vietnam Lawyers Magazine]. <https://lsvn.vn/du-lieu-ca-nhan-cua-hon-66-nguoi-dung-internet-bi-su-dung-trai-phiep-trong-nam-2024-a151492.html>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
- Nguyễn, Đ. B. (2021). Bảo vệ dữ liệu cá nhân người dùng mạng xã hội trong bối cảnh hội nhập quốc tế [Protecting the personal data of social network users in the context of international integration]. Tạp chí Phát triển Khoa học và Công nghệ – Kinh tế-Luật và Quản lý [Science and Technology Development Journal – Economics, Law and Management], 5(3), 1764–1771.
- Nguyễn, G. T. (2024). Thực trạng về vấn đề bảo vệ dữ liệu cá nhân, kinh nghiệm một số quốc gia, khu vực và đề xuất hoàn thiện pháp luật ở Việt Nam hiện nay [Current status of personal data protection, experiences of selected countries and regions, and recommendations for improving Vietnamese law]. Tạp chí Công thương [Industry and Trade Magazine], (12), 73–75.
- Nguyễn, N. T., Đặng, V. M. H., Nguyễn, D. M. T., & Ngô, H. L. (2025). Đảm bảo quyền riêng tư cho người chưa thành niên trong quá trình giám sát điện tử ngoài cộng đồng: Kinh nghiệm quốc tế và bài học cho Việt Nam [Ensuring the right to privacy of minors during community-based electronic monitoring: International experience and lessons for Vietnam]. Tạp chí Giáo dục & Xã hội [Journal of Education and Society], (Kì 1, tháng 4), 326–330.
- Phạm, T. D. T., & Phan, T. L. H. (2020). Hoàn thiện quy định của pháp luật về bảo vệ quyền riêng tư của trẻ em [Improving legal provisions on the protection of children's right to privacy]. Tạp chí Nghiên cứu lập pháp [Legislative Studies Journal], 16(416), 18–27.
- Quốc hội [National Assembly of Vietnam]. (2016). Luật Trẻ em số 102/2016/QH13 [Law on Children No. 102/2016/QH13].
- Quốc hội [National Assembly of Vietnam]. (2024). Luật Bảo hiểm xã hội số 41/2024/QH15 [Law on Social Insurance No. 41/2024/QH15].
- Quốc hội [National Assembly of Vietnam]. (2025). Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 [Law on Personal Data Protection No. 91/2025/QH15].
- Tạ, T. B. N., & Nguyễn, K. T. (2022). Tiếp cận dựa trên quyền riêng tư trong chính sách bảo vệ dữ liệu cá nhân trên các nền tảng dịch vụ công trực tuyến ở Việt Nam hiện nay [A privacy-based approach to personal data protection policy on online public service platforms in Vietnam]. VNU Journal of Science: Policy and Management Studies, 38(3), 95–105.
- Thái, T. T. D. (2012). Quyền tiếp cận thông tin và quyền riêng tư ở Việt Nam và một số quốc gia [The right to access information and the right to privacy in Vietnam and selected countries]. Vietnam National University Ho Chi Minh City Press.
- Thế Lâm. (2021). 80% nguyên nhân gây lộ lọt thông tin, dữ liệu cá nhân do người dùng bất cẩn [80% of causes of personal information and data leaks stem from user negligence]. Báo Lao động [Lao Động Newspaper]. <https://laodong.vn/kinh-doanh/80-nguyen-nhan-gay-lo-lot-thong-tin-du-lieu-ca-nhan-do-nguoi-dung-bat-can-972892.lido>
- Thủ tướng Chính phủ [Prime Minister of Vietnam]. (2025). Quyết định số 69/QĐ-TTg về việc liên thông điện tử dữ liệu khám bệnh, chữa bệnh, dữ liệu dân cư, dữ liệu hộ tịch để giải quyết hưởng chế độ ốm đau, thai sản [Decision No. 69/QĐ-TTg on the electronic interconnection of medical examination and treatment data, population data, and civil status data for the processing of sickness and maternity benefits].
- VietTimes. (2020). Lỗ hổng số hóa bệnh viện: Khi dữ liệu bệnh nhân bị biến thành món hàng [Vulnerabilities in hospital digitalization: When patient data becomes a commodity]. <https://viettimes.vn/lo-hong-so-hoa-benh-vien-khi-du-lieu-benh-nhan-bi-bien-thanh-mon-hang-post142079.html>
- Vũ, C. G., & Lê, T. N. T. (2020). Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam [Protection of the right to personal data in international law and the laws of selected countries: Reference value for Vietnam]. Tạp chí Nghiên cứu lập pháp [Legislative Studies Journal], 9(409), 55–64.