AI and Data Science Journal
Online ISSN: 3078-7394
DOI: https://doi.org/10.61784/adsj3042

TIERED CLASSIFICATION AND REGULATION OF CROSS-BORDER PERSONAL HEALTH DATA FLOWS: THE "NATIONAL SECURITY THRESHOLD" AS A REGULATORY BOUNDARY

ZhaoXia Deng
Guangdong University of Foreign Studies, Guangzhou 510515, Guangdong, China.

Abstract: Cross-border flow of personal health data has become a structural requirement in cross-border telemedicine, international multicenter clinical trials, and international collaborative research on genetic data. However, once genetic data, population health maps, and other data are maliciously utilized, they may endanger biological and national security, and the legitimacy of regulation is beyond doubt. The question is not whether to regulate, but what standards to regulate. The current regulations in China place personal health data under both the concepts of "important data" and "sensitive personal information", but both have threshold ambiguity in the field of health: the important data directory is missing, and the rules for sensitive personal information replace "national security relevance" with "sensitivity", resulting in a lack of corresponding relationship between review intensity and national security risks. There is a lack of systematic analysis on the triggering conditions for national security review in the context of personal health data, with existing research focusing on institutional comparisons outside the domain or macro construction of general cross-border data flows. This article uses the "national security threshold" as an analytical tool, defining it as a critical set of conditions for data type threshold and flow scenario threshold. It advocates for the typification and reconstruction of health data within the current three-level framework of "core data important data general data", with national security relevance as the priority axis: core types (human genetic resource information, major infectious disease pathogen genome data, population health vulnerability map) enter the scope of national security review, important types (identifiable personal diagnosis and treatment data) use security assessment as the core process, and general types (de identified statistical data and health management data) apply the facilitation path. On this basis, scenario calibration is carried out with "purpose receiver purpose" as the variable, and the functional differentiation of safety assessment, standard contracts, and national security review is divided into procedural guarantees, supported by regional testing, technical governance, and international scenario integration. The clarification of thresholds is not a weakening of the security bottom line, but a prerequisite for the legitimacy and effectiveness of national security reviews and the predictable compliance path for international cooperation in digital healthcare.
Keywords: Personal health data; Cross-border flow; Tiered classification; National security threshold

1 INTRODUCTION

The scenarios of cross-border telemedicine, international multi-center clinical trials, international collaborative research on genetic data, and cross-border transmission of wearable device data have made the cross-border flow of personal health data a structural requirement for the development of digital healthcare. A research report shows that in 2020, it was discovered that domestic genetic data was exported over 7.17 million times through the internet, and non-desensitized medical imaging data was exported nearly 400000 times [1]. This data indicates that cross-border flows have become a reality rather than an option. At the same time, if genetic data, population health maps, and other data are maliciously exploited, it may endanger biological and national security, and the legitimacy of regulation is beyond doubt. The question is not whether to regulate, but what standards to regulate.

In terms of the current regulatory framework in our country, a regulatory system that responds to this standard issue has been initially formed - with the "Data Security Law", "Personal Information Protection Law", "Data Export Security Assessment Measures", and "Regulations on Promoting and Regulating Cross border Data Flow" as the core, health data falls within the scope of both "important data" and "sensitive personal information" concepts. But both concepts have threshold ambiguity in the context of health data. In terms of "important data", the identification criteria lack refinement in the health field: whether all identifiable personal health data constitutes important data, and whether height and weight data and genetic data should be subject to the same review intensity are not answered by current regulations. In practice, the data management department and the medical industry management department have not yet formulated a specific directory of important data in the pharmaceutical field, and the national unified rules for identifying important data have not been implemented. Therefore, there are significant difficulties in the self-identification of important data. As for "sensitive personal information", the "separate consent" rule faces the practical dilemma of consent fatigue and generalized authorization in cross-border scenarios, and "sensitive" and "involving national security" are two different regulatory dimensions - using sensitivity as a review threshold instead of national security relevance may result in a mismatch of regulatory resources.

The lack of threshold values at the normative and practical levels has not been fully addressed in existing research. Existing research has focused on the adequacy assessment of extraterritorial systems such as the EU GDPR [2], the de identification pathway of the US HIPAA [3], Australia's strict restrictions on identifiable personal health data, or the

© By the Author(s) 2026, under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0).

macro institutional construction of general data cross-border flows [4]. The systematic analysis of the core issue of "triggering conditions for national security review" in the context of personal health data is still insufficient. Research has clearly pointed out that there are problems with the cross-border flow system of health and medical data in China, such as the lack of a hierarchical classification system and the intersection and redundancy of outbound regulations [5]. This article uses the "national security threshold" as an analytical tool to attempt to answer: which data types and flow scenarios in the cross-border flow of personal health data touch on the core interests of national security and should be subject to strict scrutiny, which only involve general security risks and can be applied to facilitation paths, and how this distinction can be transformed into actionable hierarchical classification regulatory rules.

2 THEORETICAL JUSTIFICATION AND FUNCTIONAL POSITIONING OF "NATIONAL SECURITY THRESHOLD"

2.1 National Security Attributes of Personal Health Data: From Individual Sensitive Information to National Strategic Resources

Health data carries multiple legal interests such as personal interests, public interests, and national security. Personality attributes are reflected in their association with personal dignity and privacy rights; The public attribute is reflected in the public value of public health governance and medical research; The national security correlation is mainly reflected in specific data types such as genetic data, population health maps, and major infectious disease monitoring data. Life and health big data is positioned as an important foundational resource for national population health and biosafety, and its governance directly relates to the maintenance of national data sovereignty [6]. Genomic data has a dual characteristic of being uniquely identifiable for individuals and possessing inherent collectivity for families and ethnic groups. Its risk types include not only individual privacy infringement, but also group level damage and bioterrorism threats [7]. The overall risk boundary of health and medical big data has been considered to go beyond the scope of individual private rights and rise to the level of national sovereignty, security, and public interest distribution [8]. Article 4 of the Data Security Law clearly stipulates that "maintaining data security should adhere to the overall national security concept", providing a direct normative basis for the national security attributes of health data; Article 85 (8) of the Biosafety Law includes "data and other information generated from the use of human genetic resources" in the scope of human genetic resources, providing a cohesive basis for the protection of specific types of genetic data and other information within the framework of biosafety risk prevention. However, "having national security relevance" does not mean that "all health data exports pose a threat to national security". From attributes to regulations, a "threshold" filtering is required: national security review is only legitimate when a specific data type substantially touches on the core interests of national security in a specific flow scenario. Universal review that does not differentiate between data types and scenarios goes beyond the necessary limits of the proportionality principle and can also result in misallocation of review resources. Of course, the purpose of classification and grading is not to include all data with national security relevance in the highest intensity regulation, but to match differentiated protection measures based on the degree of relevance on the basis of identifying national security relevance [9].

2.2 Definition and Function of the Concept of "National Security Threshold"

The national security threshold is not an existing legal concept, but a tool category constructed in this article to analyze the regulation of cross-border flow of health data. It refers to the critical set of conditions that trigger national security reviews in the cross-border flow of personal health data, including data type thresholds (which data are related to core national security interests in nature) and flow scenario thresholds (under what purpose, recipient, and use, the export of the data constitutes national security risks). The normative basis for this definition lies in the fact that the identification of "important data" in current law itself requires substantive judgment based on the domain attribution, group coverage, accuracy scale, and affected objects of the data. The national standard clearly states that "data that only affects the organization itself or individual citizens is generally not considered important data" [10], which means that there is no automatic equivalent relationship between "identifiable personal information" and "important data", and it needs to be filtered by the substantive objects of influence. However, the reality in the field of health and medical data is that the absence of a hierarchical classification system and an important data directory makes this substantive filtering lack an operable carrier, and security assessments have to be judged on a case-by-case basis [5]. In this sense, the function of the "national security threshold" is to establish operational judgment criteria between the existing concepts of "important data" and "sensitive personal information", and to shift the classification of national security review from the form of "whether it belongs to important data" to the substantive judgment of "whether it substantially touches on the core interests of national security in specific scenarios". This shift is consistent with the inherent logic of data classification and grading protection: the purpose of classification and grading is to "determine the level of security protection that matches the category and level" [9], rather than including all data related to national security in the highest intensity regulation. Therefore, the threshold is not a reduction in national security standards, but a precise targeting of the objects of review –concentrating limited review resources on data types and flow scenarios that truly concern national security, while releasing institutional space for the flow of health data that does not touch the threshold.

3 REVIEW OF THE CURRENT STATUS OF GRADED AND CLASSIFIED REGULATION OF CROSS-BORDER FLOWS OF PERSONAL HEALTH DATA IN CHINA

3.1 Graded and Classified Elements in the Current Regulatory System

The current standards already include several grading and classification elements. Article 21 of the Data Security Law establishes a three-level framework of "core data important data general data". Article 28 of the Personal Information Protection Law classifies medical and health information as sensitive personal information. The "Guidelines for Health and Medical Data Security in Information Security Technology" (GB/T 39725-2020) classifies health and medical data into five levels based on "data importance, risk level, and potential harm and impact on individual health and medical data subjects", with the fifth level being "data that is only available for access and use within a very small range and under strict restrictions". The "Measures for Security Assessment of Data Export" trigger security assessments based on "key information infrastructure operators," "important data," and "sensitive personal information quantities". After the implementation of the Personal Information Export Authentication Measures, the three paths established in Article 38 of the Personal Information Protection Law, namely security assessment, standard contract filing, and personal information protection authentication, have all been fully implemented, and data export supervision has entered the "three track parallel" stage [11]. But these classification elements serve different purposes: the five-level classification of GB/T 39725-2020 serves to match domestic circulation and security measures, sensitive personal information rules serve to protect individual rights and interests, and security assessment triggering conditions serve to control outbound risks. There is a lack of logical connection among the three based on the unified anchor point of "national security relevance", and the "level" of the same health data in different regulatory systems may not correspond.

3.2 Practical Dilemmas: An Examination from the Perspective of "National Security Threshold"

The current tiered and classified regulation of cross-border flow of personal health data exhibits structural gaps at the levels of standards, procedures, and systems. These three aspects are not independent issues in parallel, but rather represent systemic cruxes that unfold layer by layer in terms of procedural operation and organizational support, with "standard absence" at their core.

First of all, there is a lack of standards and grading criteria centered around national security relevance. This deficiency is evident at both normative levels. In terms of identifying important data, the Data Security Law requires the establishment of an important data directory, but the important data directory for the health and medical fields has not yet been introduced. Industry surveys have shown that the lack of a scientifically reasonable data classification and grading system has become an important factor hindering the practical exploration of the elementization of health and medical data [12]. Lu Yu and Yang Xiangyu also listed the "lack of a grading and classification system" as a prominent problem in cross-border mobility systems [5]. Another study has pointed out that the "lack of object classification" inhibits the utilization efficiency of personal health data space [13]. The absence of a directory leads to two biases: if all identifiable personal health data is included in the important data category, all such data must undergo security assessments for export, creating a tension between compliance costs and review capacity; If no distinction is made in essence, data types such as genetic data that truly touch the core of national security may not be effectively locked in due to unclear thresholds. As for the existing grading standards, the five-level classification of GB/T 39725-2020 is based on the "potential harm and impact on personal health and medical data subjects", and the protected object is individual rights rather than national security. This benchmark creates a misalignment in two directions in cross-border scenarios: data with lower sensitivity at the individual level (such as population disease statistics, regional health resource data) may have higher correlation at the national security level due to the involvement of population health vulnerability analysis; Genetic data belongs to level 5 in the individual dimension, but whether its national security relevance needs to match the same level of exit review intensity cannot be directly derived from individual classification. Scholars have proposed a "dynamic classification and grading framework based on the scenario theory" to compensate for the shortcomings of static grading, which precisely illustrates the fact that existing grading has not yet incorporated national security variables in cross-border scenarios into the judgment structure [5]. The key to the problem is not whether a directory has been established, but whether a threshold standard centered on national security relevance has been established behind the directory and classification, so that identification can lock in core data types without over covering general data.

Secondly, the program lacks data and path selection lacks typification guidance based on data types and scenarios as variables. Article 38 of the Personal Information Protection Law establishes three exit paths: security assessment, standard contract filing, and personal information protection certification. After the implementation of the Personal Information Exit Certification Measures on January 1, 2026, all three paths will be fully implemented, and data export supervision will enter the "three track parallel" stage [11]. But in the field of personal health data, the applicable boundaries of the three paths overlap. The triggering conditions for security assessment are centered on the quantity of "important data" and sensitive personal information, while standard contracts and certifications apply to situations where the cumulative number of sensitive personal information leaving the country has not reached the threshold of 10000 people. However, when a certain type of health data has a high degree of national security relevance but the cumulative outbound quantity has not yet reached the evaluation threshold, path selection lacks typological guidance based on data types and scenarios as variables. The essence of this dilemma lies not in the unclear design of the three paths themselves, but in the fact that the threshold standard for "what kind of data should be mandatory for security assessment" has not yet been implemented in the health field. The rules of the negative list of Beijing Free Trade Zone provide a comparison: according to the "Rules Table for Determining Health Data Levels", data that is deemed to have caused serious damage to national security or above, even if the annual number of outbound people is less than 50000, cannot be subject to standard contract filing or

certification [14]. In the view of this article, this design is an attempt to introduce national security impact as the substantive triggering condition beyond the quantity threshold, but its connection with the national level unified threshold standard still needs to be clarified.

Thirdly, the system is unclear and there is a lack of procedures to connect professional judgment with safety review. Article 10 of the "Measures for Security Assessment of Data Export" stipulates that the national cyberspace administration department shall "organize relevant departments of the State Council, provincial cyberspace administration departments, specialized agencies, etc." to conduct security assessments after accepting the application. However, the specific direction of "specialized agencies" and their relationship with the health authorities are not clear. Although expert consultation can be introduced in evaluation practice, leaving room for flexibility in professional judgment, there has not yet been an institutionalized connection with the health regulatory authorities. The connection mechanism between professional judgment of health data (data type identification, risk assessment of clinical and scientific research scenarios, ethical review) and comprehensive judgment of data security review (outbound purpose, recipient protection level, national security impact) lacks procedural arrangements in current standards. In the absence of a unified threshold standard centered on national security relevance, it is difficult for professional departments and security review departments to form a shared judgment benchmark on "what data, in what scenarios, and with what intensity of review", making it difficult to clarify the division of responsibilities.

3.3 The Essence of the Problem

The common root cause of the above difficulties lies in the lack of standards: the current rules use "whether it belongs to important data/sensitive personal information" as the review entry point, but both lack substantive judgment rules based on "national security relevance" in the field of health, and the classification and grading remain in formal classification, without establishing a three-dimensional judgment framework of "data type flow scenario national security risk". The lack of program data and unclear system is a manifestation of the absence of standards in the operation of the system: when the threshold is not determined, the path selection loses its stable premise; Without shared judgment criteria, it is difficult to clarify the boundaries of responsibilities. The three factors collectively lead to a lack of correlation between the intensity of censorship and national security risks. Reconstructing hierarchical and classified supervision with the "national security threshold" as the anchor point is precisely providing a unified judgment axis for existing standards, procedures, and systems.

4 COMPARISON AND ENLIGHTENMENT OF OVERSEAS EXPERIENCE

4.1 EU: Classification Model Based on the Threshold of "Adequacy Protection"

Article 9 of GDPR generally prohibits the processing of personal health data, with exceptions limited to statutory circumstances such as public interest, medical purposes, and scientific research; Articles 45-49 provide a three-tier pathway for cross-border transfers: adequacy determination (Article 45), appropriate safeguard measures (Article 46, including standard contract terms and binding company rules), and specific circumstances mitigation (Article 49). The essence of adequacy determination is to require third countries to provide an "essentially equivalent" level of data protection, and its judgment object is the overall protection level of the destination legal order, rather than the data type itself [15]. EHDS has further established a hierarchical governance structure for the initial and secondary utilization of health data within the GDPR framework. Secondary utilization requires approval from the Health Data Access Board (HDAB) established by each member state, which evaluates the purpose, necessity, and legal basis of the application and issues a data license. The license is valid for a maximum of ten years and can be extended once [16]. The core logic is to use "whether the level of destination protection is sufficient" as the cross-border threshold, and the internal classification of personal health data is mainly achieved through the use of purpose stratification (primary/secondary utilization) and access control procedures, rather than using the data type itself as an independent threshold. It can be seen that the adequacy recognition mechanism provides an institutionalized channel for the flow of health data to countries with equivalent levels of protection, but this mechanism is mainly reflected in the overall recognition at the national level in practice. Although adequacy determination can legally cover "a country as a whole or its specific sectors", academia has long advocated for sectoral adequacy determination targeting the health sector [17]. However, sectoral adequacy determination has not yet become the norm in practice, and the response to differentiated needs within different levels of health data is limited.

4.2 United States: Free Flow Model with "De-identification" as Threshold

HIPAA protects "protected health information" (PHI), which refers to health information that identifies individuals. De-identified data, those removing 18 types of identifiers according to the "safe harbor" standard, or re-identifying with extremely low risk as determined by experts, no longer constitutes PHI and is therefore not restricted by HIPAA privacy rules for use and disclosure, nor is it hindered by HIPAA in cross-border scenarios [18]. At the cross-border level, the United States achieves the cross-border flow of personal data (including health data) through the APEC Cross Border Privacy Policy (CBPR) certification mechanism, based on corporate accountability. CBPR requires companies to entrust APEC certified assessment agencies to conduct privacy impact assessments, which clearly include whether the processing policies for sensitive information such as personal health data comply with protection requirements [19]. The core logic

is to use "recognizability" as the regulatory threshold: recognizability means being constrained by PHI rules, and de identification means breaking free from these constraints. Therefore, the de-identification threshold frees up space for data utilization, but the assumption that "de-identification is safe" does not hold true for some data types. Empirical studies have shown that even datasets processed according to HIPAA safe harbor standards still face re identification risks, and reporting rates vary depending on data types and attack methods [20]. The re-identification risk borne by vulnerable groups such as rare disease patients is particularly prominent. In addition, the scope of application of HIPAA is limited to "covered entities" and their business partners. Health data collected by non-covered entities such as health applications is not within its scope, and the regulatory model based solely on recognizability threshold is difficult to cover the entire health data ecosystem.

4.3 Australia: Strict Restriction Mode Based on "Identifiable Personal Health Data" Threshold

Article 8 of the Australian Privacy Act requires data disclosure entities to take reasonable measures to ensure that the recipient does not violate Australian Privacy Principles (APPs) before disclosing personal information to overseas recipients, and to hold the disclosing entity responsible for any improper handling by the recipient; Exceptions include personal consent, legal requirements, and legal constraints that are substantially similar to APPs [21]. In terms of personal health data, Article 77 of the My Health Records Act sets stricter rules: operators of MHR systems, registered repository operators, and other entities are not allowed to hold or process information related to MHR records outside of Australia; The exception is only applicable to system operators who process data outside the country for the purpose of operating or managing the MHR system, which does not include personal information of healthcare recipients or participants, nor does it include identifying personal or entity information. Violators face criminal penalties, up to a maximum of 5 years in prison or 300 penalty units, or both. The core logic is based on the threshold of "identifiable personal health data", which is generally prohibited from leaving the country within the MHR system, with extremely limited exceptions reserved only on the premise of not containing identifiable information. It can be seen that the strict restrictions on identifiable personal health data in the Australian model effectively reduce national security risks, but overly strict localization measures have also been questioned by the industry. Microsoft has pointed out to the Australian government that the requirement to store electronic health records domestically is a "structural weakness" that may have adverse effects on security, and physical location itself does not necessarily enhance data security [22]. In addition, in the *Privacy Commissioner v. Telstra Corporation Limited*, the federal court provided a restrictive interpretation of "recognizability", clarifying that "personal information" is limited to information about individuals, and that linkability alone is not enough to make it personal information [23]. This indicates that the threshold standard itself is not fixed and needs to be dynamically adjusted according to technical conditions and judicial interpretations.

4.4 Comparative Analysis and Implications for China

All three modes use a certain "threshold" as the logical starting point for hierarchical classification: the EU uses "adequacy of destination protection level" as the threshold, the United States uses "recognizability" as the threshold, and Australia uses "identifiable personal health data" as the threshold. Their common limitation lies in the relatively single threshold dimension: the EU model mainly focuses on the overall level of protection of the destination legal order, the US model mainly focuses on whether the data can identify individuals, and the Australian model chooses the regulatory strength of "principle prohibition" on the same "identifiability" threshold. None of the three have institutionalized the correlation between data types and national security as a hierarchical dimension independent of identifiability. The institutional context of our country: the overall national security concept, the classification and grading framework of Article 21 of the Data Security Law, and the lack of specialized regulations in the field of health data, requires a composite threshold framework that includes three-dimensional variables of data types, flow scenarios, and national security risks in addition to "identifiability" and "adequacy of protection level".

5 A TIERED CLASSIFICATION REGULATORY FRAMEWORK CENTERED ON THE "NATIONAL SECURITY THRESHOLD"

5.1 Grading Criteria: Typification Reconstruction Centered on National Security Relevance

The current system has provided a preliminary administrative framework for the classification and grading of personal health data. On February 14, 2026, the National Health Commission and other departments jointly issued the "Management Measures for Data Security and Personal Information Protection of Medical and Health Institutions (Trial)" (National Health Planning [2026] No. 6), which divides medical and health institution data into three categories: core data, important data, and general data. Institutions are required to conduct data asset inventory, identify important and core data, and submit them to local health administrative departments. Provincial health administrative departments will coordinate the classification and grading of medical and health institution data and propose directory recommendations. This method also clarifies that "personal information may constitute important data when it reaches a certain level of accuracy and scale", and encourages the promotion of data utilization through the method of "original data not leaving the domain, data available but not visible" [24]. However, the identification logic of this framework still relies mainly on data management dimensions (source, category, scale, accuracy), and the national security relevance has not yet been established as an independent hierarchical axis that takes priority over data management dimensions. The consequence is

that data types that truly touch on biosafety and population security, such as genetic data, major infectious disease monitoring data, and population health vulnerability maps, may be placed under the same category of "important data" as general identifiable individual diagnosis and treatment data, and the intensity of review cannot reflect the differences in risk nature; However, some data with low sensitivity in the dimension of individual rights but high correlation in the dimension of national security (such as regional population disease susceptibility statistics, pathogen genome sequences) may not be effectively identified due to the "scale" or "accuracy" of the data management dimension not meeting the threshold.

Therefore, this article advocates for the typological reconstruction of health data within the current three-level framework, with national security relevance as the priority axis. Firstly, the core type refers to data that, once exported, may be used for biological weapon development targeting specific ethnic groups, population health vulnerability analysis, or information advantage acquisition in strategic competition. Human genetic resource information (genome sequence, specific gene locus variation data) is subject to dual constraints of the Regulations on the Management of Human Genetic Resources and the Biosafety Law. Its export must be approved or filed by the human genetic resource management department, and the security assessment of the cyberspace administration department operates independently as a parallel program [25]. The genomic data of major infectious disease pathogens and early warning data of epidemics are related to public health emergency response capabilities, while the population health vulnerability map involves population security. The national security correlation between the two is on the same level as genetic data. The regulatory logic for such data should not be limited to the general security assessment of "important data", but should enter the scope of national security review. In principle, it is prohibited to leave the country, and exceptions must be approved through review. Secondly, important types refer to identifiable personal medical data such as electronic medical records, medical imaging, test results, medication records, etc. The risk nature of such data mainly involves individual rights and public interests, with a moderate degree of national security relevance. Its export is based on security assessment as the core procedure, and standard contracts and separate consent as supporting conditions. Thirdly, the general type refers to de identified statistical data, medical management data, health resource data, and publicly available health science popularization data, which have low national security relevance and can be facilitated through standard contract filing or protection certification. It also explores mutual recognition mechanisms between countries or regions whose protection levels have been assessed and recognized. The boundaries between the three layers are not fixed and unchanging: changes in the effectiveness of de identification techniques, the expansion of data aggregation scale, and the emergence of new pathogen information may all move a dataset from general types to important types, and even touch on core types. Therefore, grading is not a one-time classification, but should be embedded with a dynamic adjustment mechanism. The health regulatory department, in conjunction with the internet information department, should regularly evaluate the correspondence between data types and national security relevance based on the current directory submission mechanism.

5.2 Scenario Calibration: Intensity Adjustment with "Purpose Receiver Purpose" as a Variable

The classification of data types is based on baseline strength, and scenario-based review is calibrated on this basis. Its function is not to change the level to which the data type belongs, but to determine the specific configuration of the review program within the same level. In the context of scientific research cooperation, international multi-center clinical trials and cross-border academic research are based on public interest and ethical review as legitimacy. Important types of data can be subject to a combination of informed consent, ethical review, and safety assessment, while core types of data require approval from science and technology regulatory authorities in addition to national security review. The experience of the COLOR III project at Beijing Friendship Hospital shows that professional judgment in safety assessment needs to cover the scientific significance of the research project, the necessary correlation between data export and project implementation, and the security capabilities of overseas recipients [5]. In cross-border diagnosis and treatment scenarios, remote consultation and cross-border referral are centered on patient interests, and important types of data can be simplified by combining individual consent and standard contracts. Core types of data are generally not included in this scenario, except for emergency treatment situations that have been approved by the health regulatory authorities. In commercial utilization scenarios, health application data and insurance actuarial data are based on de identification. Generally, certification or standard contracts are applicable to general types of data, while important types of data must undergo security assessments and overseas recipients must have a protection level equivalent to that of China. Emergency procedures are applicable in public health emergency scenarios, and procedures can be completed afterwards, but the scope and duration of data use must be strictly limited. After the event is over, the data must be deleted or returned within a specified time limit. The normative significance of scenario calibration lies in the fact that the national security risks of the same data type in different scenarios are not the same. Adjusting program configuration based on scenarios as variables can better achieve the correspondence between review intensity and risks than a one size fits all approach with a single threshold.

5.3 Program Layering: Functional Differentiation of Security Assessment, Standard Contracts, and National Security Review

The program mechanism should match the results of data type and scenario calibration, rather than simply "choosing" between the three outbound paths. For data that touches on core types, national security review is an independent and pre requisite process and cannot be replaced by general security assessments. The review is coordinated by the cyberspace

administration department, with professional opinions on data type determination and risk level provided by the health regulatory department. National security agencies make judgments on whether data export may endanger biological safety, population security, or information advantages in strategic competition. For important types of data, security assessment is the core procedure, focusing on reviewing the security capabilities of overseas recipients, the specificity and necessity of data usage purposes; Standard contracts must include usage scope limitations, re transfer restrictions, security incident notifications, and deletion and return clauses; Individual consent must be communicated in clear and understandable language regarding the purpose of departure, data type, recipient identity, and risks. For general types of data, standard contract filing or protection certification can meet compliance requirements. The institutional premise of program stratification is the operability of identification criteria: only when the boundary between core types and important types can be reasonably judged by data controllers in advance, can program selection not degenerate into uncertainty avoidance. The Beijing 2025 version of the negative list will expand the management mechanism from free trade zones to the entire provincial administrative region, and add new fields such as medical devices, forming a "1+9" list system (9 industry fields, 67 business scenarios, 612 fields) [26], indicating that local levels are accumulating program configuration experience based on data types and scenarios, but these experiences still need to be connected with national threshold standards.

5.4 Supporting System: Cautious Promotion of Regional Trials, Technological Governance, and International Integration

Regional pilot testing should shift from "institutional declaration" to "validation of replicable rules". Under the framework of the *Implementation Guidelines for Cross border Personal Information Flow Standard Contracts in the Guangdong Hong Kong Macao Greater Bay Area (Mainland China, Hong Kong Region)*, Zhongshan City has established the first compliant cross-border commercial insurance claim scenario for Hong Kong *Region's* residents in the province. When Hong Kong *Region's* residents seek medical treatment at Zhongshan Chen Xinghai Integrated Traditional Chinese and Western Medicine Hospital, they receive authorization and consent to have their diagnosis and treatment data legally exported through a secure encrypted channel in a trusted data space, automatically completing underwriting and claims, and achieving the landing from "data transmission" to "business closed loop" [27]. This scenario has completed the standard contract filing in terms of system, establishing the rule of "data is only for use in claims verification, non-secondary circulation, and not transferred to third parties". Hong Kong *Region* insurance institutions only obtain the minimum dataset necessary for claims verification; Technologically integrating "national secret algorithm + privacy computing + blockchain" to ensure the security and controllability of the entire process. The core value of these practices lies not in "opening up", but in testing whether the program configuration with data types and scenarios as variables is operable under the conditions of "one country, two systems, and three legal domains". There have been academic explorations on the application of privacy computing and federated learning in cross-border health data cooperation, such as the Plug system discussing the conditions and limitations of federated learning in balancing FAIR principles, compliance, and network security in medical scenarios. However, its institutionalization is based on the premise that the technical effectiveness can be independently evaluated and the evaluation results can be accepted by the reviewing authorities - the technical solution itself cannot replace legal threshold judgments, but can only be used as a means to meet the review requirements [28]. At the level of international rule docking, RCEP and DEPA provide a framework arrangement for cross-border data flow, but the national security dimension of health data makes mutual recognition not based solely on "sufficiency" or "free flow". A more cautious approach is to explore scenario-based arrangements based on mutual recognition of national security thresholds in specific, recipient limited, and time limited scenarios such as public health emergency data sharing and international multicenter clinical trials, rather than promoting comprehensive mutual recognition at the general health data level.

6 CONCLUSION

The regulatory challenge of cross-border flow of personal health data lies not in whether there is a tension between "security" and "flow", but in the fact that the current system has not yet provided a set of judgment standards that correspond the intensity of review with national security risks. This article uses the "national security threshold" as an analytical tool, advocating for the use of national security relevance as a baseline, mobile scenarios as calibration variables, and program stratification as institutional safeguards within the current three-tier framework. The review resources should be focused on data types and scenarios that truly touch on biosafety and population security, such as genetic data, major infectious disease monitoring data, and population health vulnerability maps. At the same time, expected compliance space should be released for the flow of health data that does not touch the threshold. The feasibility of this framework depends on the operability of identification standards, the procedural coordination between professional judgments of health regulatory authorities and security reviews by cyberspace administration and national security reviews, as well as the institutionalization of "available invisible" technology governance. Technical solutions cannot replace legal threshold judgments. The argument of this article starts with the analytical construction of the "national security threshold", which still has limitations in the boundaries between important and general types, the coverage of countries compared outside the domain, and the mechanism of technology and legal connection. However, the clarification of the threshold itself does not weaken the security bottom line. It is precisely the prerequisite for the legitimacy and effectiveness of national security review and the predictable compliance path for international cooperation in digital healthcare.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This work is supported by the Characteristic Innovation Project of Guangdong Regular University [Grant: 2023WTSCX023].

REFERENCES

[1] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). 2020 China Internet Network Security Report, 2021.
[2] Ao Q, Pan Y. The EU Experience in the Cross-Border Flow of Personal Health and Medical Data and Its Implications. Medicine and Philosophy, 2025, 46(23): 19-24.
[3] Chen Y Y, Meng Y C. Research on the Legal Regulation of the Cross-Border Flow of Health and Medical Data in Australia and Its Implications for China. Chinese General Practice, 2024, 27(25): 3091.
[4] Jiao Y, Ji J H. Practical Review and Multidimensional Construction of Norms for Cross-Border Data Flow. Journal of Xi'an University of Finance and Economics, 2026, 1: 68.
[5] Lu Y, Yang X Y. Current Regulatory Status and Solutions to the Dilemmas of Cross-Border Flow of Health and Medical Data in China. Medicine and Jurisprudence, 2025.
[6] Bao Y M, Xue Y B. Current Status and Prospects of Life and Health Big Data. Bulletin of the Chinese Academy of Sciences, 2018, 33(8): 861-865.
[7] Wang G. Towards equitable governance of human genomic data sharing: guided by genomic contextualism. Data & Policy, 2025, 7: e83.
[8] Yang J M, Fang Y, Kuang Y L, et al. Legal Risks and Regulatory Pathways in the Application of Health and Medical Big Data. Journal of Sichuan University (Medical Science Edition), 2026, 57(3): 880-886.
[9] Hong Y Q. Data Classification and Graded Protection from the Perspective of National Security. China Law Review, 2021, 5: 71-78.
[10] National Technical Committee 260 on Cybersecurity of SAC (TC260). Data Security Technology—Rules for Data Classification and Grading. GB/T 43697-2024, 2024.
[11] Xu Z Y, Wang Q. The Full Picture of Compliance Pathways for Outbound Pharmaceutical Data: Scenario Identification and Practical Responses from Clinical Trials to Pharmacovigilance. Zhonglun Wende, 2026. https://www.zhonglunwende.com/index.php/zhuanyewenzhang/3731.html.
[12] Deng X H, Ye J Q, Liang M B, et al. Research on the Dilemmas and Countermeasures in the Elementalization of Health and Medical Data. Chinese Journal of Digital Medicine, 2025, 20(6): 24-29.
[13] Zhao F. On the Legal Guarantees for the Construction of a Trusted Health Data Space in China. Journal of University of Electronic Science and Technology of China (Social Sciences Edition), 2025, 27(6): 112-121.
[14] Duan Z C, Wang Y T, Xu L, et al. A Thousand Mountains Layered like Zhang, a Hundred Rivers Flowing to the Sea: An Interpretation of the Negative List for Outbound Data Transfer in the Beijing Pilot Free Trade Zone (Part II). Hankun Law Offices, 2024. https://www.hankunlaw.com/portal/article/index/cid/8/id/14576.html.
[15] Chen Y M, Ji Z T. The Twin Drivers in Constructing Discursive Power in EU Digital Trade Rules: The Resonance between Unilateral "Adequacy Decisions" and Bilateral Trade Agreements. German Studies, 2025, 6: 92-95.
[16] Regulation (EU) 2025/327 on the European Health Data Space, 2025, arts 57, 68.
[17] Bentzen H B, Castro R, Fears R, et al. Remove Obstacles to Sharing Health Data with Researchers Outside of the European Union. Nature Medicine, 2021, 27(8): 1329-1333.
[18] US Department of Health and Human Services. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule. HHS, 2012. https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html.
[19] Asia-Pacific Economic Cooperation (APEC). Cross-Border Privacy Rules System. APEC, 2011. https://cbprs.org/.
[20] Tovino S A. Not So Private. Duke Law Journal, 2022, 71: 985.
[21] Office of the Australian Information Commissioner (OAIC). Chapter 8: Australian Privacy Principle 8 — Cross-Border Disclosure of Personal Information. Version 1.3. Office of the Australian Information Commissioner (OAIC), 2025.
[22] The Register. Microsoft to Aussie gov: Privacy rules stifle e-Health. The Register, 2011. https://www.theregister.com/offbeat/2011/11/25/microsoft-to-aussie-gov-privacy-rules-stifle-e-health/743749.
[23] Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4. 2017, 249 FCR 24
[24] National Health Commission, Ministry of Public Security, Cyberspace Administration of China, et al. Measures for the Administration of Data Security and Personal Information Protection in Medical and Health Institutions (Trial). Guo Wei Gui Hua Fa [2026] No 6, 2026.
[25] Sun Q Y, Liu Y, Huang J, et al. Management Discussion of Laws and Regulations on Human Genetic Resources in China: A Scoping Review. BMC Medical Ethics, 2026, 27: 114.

[26] Luo Q W. Data Cross-Border Flow Facilitation Reform Upgrades from “Pilot Exploration” to “City-Wide Governance”: Negative List Measures for Outbound Data Benefit Enterprises across the Municipality. Beijing Daily, 2026. https://www.beijing.gov.cn/ywdt/gzdt/202605/t20260512_4646632.html.

[27] Cyberspace Administration of China, Innovation, Technology and Industry Bureau of the Hong Kong Special Administrative Region Government. Implementation Guidelines for the Standard Contract for Cross-Border Flow of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong Region). 2023.

[28] Plug R B F. Secure Distributed Machine Learning in Healthcare: A Study on FAIR, Compliance and Cybersecurity for Federated Learning. Thesis, Leiden University, 2025. https://hdl.handle.net/1887/4285632.