Risk Management and Healthcare Policy Dovepress

Open Access Full Text Article

PERSPECTIVES

Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows

Linhua Xia[1], Zhen Cao[2], Yue Zhao[3]

[1]School of Economics, Shenzhen Polytechnic University, Shenzhen, Guangdong, People's Republic of China; [2]School of Law, Hainan University, Haikou, Hainan, People's Republic of China; [3]School of Law, Hainan Normal University, Haikou, Hainan People's Republic of China

Correspondence: Yue Zhao, School of Law, Hainan Normal University, Haikou, Hainan, People's Republic of China, Email lawzy@hainnu.edu.cn

Abstract: The growing global exchange of healthcare data requires more cohesive and effective regulatory frameworks to ensure fair access and protect patient privacy. However, cross-border regulatory rules for healthcare data diverge across countries, such as the EU, which highlights personal data rights and restricts cross-border flow of healthcare data through the GDPR, the United States, which emphasizes the free flow of healthcare data trade or services, and China, which emphasizes cross-border regulatory rules for healthcare data at the level of national data security. Such inconsistent policies often impede international medical research collaborations, undermine the effectiveness of telemedicine, and create barriers for healthcare providers to share patient information. Documents containing national human rights laws, the Global Initiative on Digital Health and the Global Digital Compact, which advocate for cooperation and behavioral co-regulation of healthcare data stakeholders to achieve the strategic goal of putting people at the center of healthcare, provide new ideas for solving the problem. Based on an exploration of these challenges, this paper proposes a harmonized, human rights-based approach that in turn bridges regulatory gaps and ensures data security, privacy, and accessibility in all countries.
Keywords: cross-border data flow, healthcare data, regulation, human rights, safety

Introduction

While cross-border flow of data refers to any type of data transfer that moves data from one country's sovereignty to another or to international/supranational organizations for processing, including import, export, and transmission of data, data cross-border policies are primarily concerned with the outflow of data.[1] The Organization for Cooperation and Development of the World Economy (OCED) estimates that data flows contribute more to global GDP than global merchandise trade and reach $2.8 trillion, growing to $11 trillion by 2025.[2] The highly uneven distribution of healthcare resources across the globe has led to the rise of telemedicine and electronic health records, cross-border medical research collaborations and healthcare needs. Telemedicine includes health data analytics and the application of big data and artificial intelligence methods in epidemiological research and diagnostic support, resulting in the generation of massive amounts of healthcare data.[3] By 2020, the global healthcare industry generates 2.3 ZB of data, but 97% of it is unutilized. If effectively utilized, this vast amount of health data could lead to more effective treatments and cures and free up scarce resources.[4]

As data traffic increases, concerns about misuse of data and inefficiencies in data storage are prevalent, as these detrimental behaviors may negatively impact national security, public morality, and the privacy rights of individuals within states. Early in the EU integration process, cross-border healthcare for citizens of EU member states gave rise to the urgency of governance of healthcare data across borders. In recent years, the EU has launched the EU Health Data Space (EHDS) initiative based on established rules, aiming to promote inter-country cooperation with a regionally harmonized regulatory framework. With the globalization of data, healthcare data cross-border occurs on a large scale between other countries. Currently, major economies are adopting increasingly stringent restrictions on data outflows,

Received: 12 October 2024
Accepted: 18 December 2024
Published: 21 December 2024

with an emphasis on data localization, but with significant policy differences.[5] This lack of international legal harmonization has led individual countries to impose domestic restrictions on cross-border data flows, which severely impacts the economy and foreign investment, and does not contribute to a unified order global data governance.[6] Indeed, there are complex competing interests behind such challenges that impede international medical research collaborations, jeopardize the effectiveness of telemedicine, and create obstructive boundaries for healthcare providers when sharing patient information.

Healthcare data is not only based on citizens' privacy and closely related to national biosecurity, but also concerns citizens' medical and healthcare rights needs, as well as recognizing and realizing the value of the international human right to life and health. Therefore, it is a test for sovereign states to find a more appropriate regulatory model to realize the balance of multiple interests on the basis of safeguarding individual rights and maintaining national security. Based on the above considerations, this paper attempts to compare different regulatory paradigms for cross-border flow of medical and health data, analyze the shortcomings in the relevant rules, and then put forward recommendations for the transformation of the regulatory paradigm and the improvement of the system centered on human rights, with a view to promoting the cross-border flow of medical and health data on a global scale.

Literature Review

Divergence Between Data Protection and Free Flow

Data protection is now a key concern in the global data legislation, but data collection itself is rarely an issue. The conceptual underpinnings of data protection are based on two competing and often conflicting goals: protecting individual privacy and promoting the free flow of information.[7] Economically, the flow of data allows for the efficient allocation of financial resources and narrows the gap between technologically and economically unequal countries.[8] The key to dealing with data crossing borders is how to ensure fairness in the subsequent use of the data and what responsibilities are imposed on the parties processing particular information, rather than imposing restrictions on data collection itself.[9] However, the free flow of data is not an absolute value, and an overemphasis on data protection laws can lead to their conflict with the basic principles of existing international fair trade legislation. Although cross-border data flows are often associated with the free flow of information, they are not the same thing, and the basic concept of information transfer is more clearly expressed by the term "international information transfer" than "cross-border data flows".[10] However, national sovereignty and individual privacy do not explain all the steps taken by countries to restrict the transmission of information outside their borders, which are more like non-tariff barriers to protect the development of their information industries.[11] For instance, in the European Union, in order to promote the development of local industries and small and medium-sized digital enterprises (SMEs) within its borders, and to protect the personal data of EU citizens, its regulation of the business of external marketplaces has become more stringent.[12] Another instance, in July 2024, the Dutch National Security Agency (NSA) imposed a €290 million penalty on YouBuy. The reason was that Uber had collected sensitive information about European drivers, but transferred this data to Uber's US headquarters without the use of a transmission tool and retained it on servers in the United States. The information relates to drivers' account information and cab licenses, but also includes location data, photographs, payment information, identification documents, and in some cases even drivers' criminal and medical data.[13] The concept of cross-border personal data transfer restrictions is not unique to the EU, and restrictions on personal data transfers and data localization requirements have sprung up.[14] That is, the The global trend is to restrict the cross-border flow of all data, including healthcare data.

Rationale and Consequences of Restricting Cross-Border Medical Data

Healthcare data has become an increasingly important component of world trade. However, the cross-border sharing of health data (and related resources) for research purposes raises particular legal issues that make it subject to specific provisions in various legal frameworks.[15] Statist controls will continue to dominate the cross-border governance of genomic data for years to come.[16] All data protection laws to some extent burden multinational corporations and others seeking to move data across borders.[17] The norms underpinning the rules for cross-border data flows may include privacy protection, protection of the public interest and national security, local economic development, the right to access

information, and the development of global e-commerce.[18] However, government policies restricting the free flow of information may have other unintended negative impacts such as reducing economic growth and discouraging innovation.[19] They can also prevent a premium on the value of cross-border flows of data, driving more industries into non-compliant operations.[20]

For healthcare providers, the exchange of patient and population health-related data between regions is critical for continued innovation in treatment and public health.[21] Data sharing between scientific organizations is critical to advancing knowledge by supporting data analysis with greater statistical power, while also validating and reproducing previously obtained results.[22] As such, they argue that the effective development of innovative tools to protect patients and prevent disease should not be unduly hindered.[23] Instead, the fragmentation of political interests between countries and weaknesses in the institutional framework for regional collective action could trigger regional health crises and even global health crises.[24] Where possible, access to scientific resources should be unrestricted and free.[25]

However, some researchers are concerned that repurposing routinely collected medical data for research is not without the risk of associated values, and may carry the risk of stigmatizing specific groups such as races of color and people with disabilities.[26] At the same time, such medical research practices may also result in subjective and objective adverse consequences of discrimination and sharing of personal information based on health data.[27] Indeed, large-scale data breaches will create significant challenges to personal privacy protection. Therefore, cross-border biomedical research management can be realized through the administrative law approach of establishing a national supervisory body to review and supervise the transfer of medical data.[28] Accountability of cross-border data flows goes hand in hand with abuse control.[29] France's National Commission on Freedom of Information (CNIL), for example, in 2022, issued a €1.5 million fine to medical software provider DEDALUS BIOLOGIE for disseminating the sensitive personal information of nearly half a million people on the Internet.[30] At the same time, Section 203 (1) paragraph 1 of the German Penal Code (StGB) criminalizes breaches of medical confidentiality, including the unauthorized disclosure of patient data to an offshore healthcare provider. Such severe sanctions will discourage doctors from providing better and more precise treatment services to their patients.

To bridge this divide, the World Health Organization (WHO) developed the National Health Regulations (2005), which not only define the criteria for "public health emergencies of international concern", but also clarify the rights and obligations of member states, and require countries to strengthen governance cooperation. However, with the rapid development of digital technology, the cross-border flow of global healthcare data based on the UN framework has long exceeded the above scope, and while political data transfer cooperation has been recognized by countries, there are still practical differences in the cross-border flow of commercial and research healthcare data.

In general, the above views discuss the regulatory basis and institutional proposals for cross-border data flows from multiple perspectives, but these views are often an "either/or" game of interests between data rights restriction and free flow, and the position is still wavering. Therefore, there is a need to find more convincing interpretative positions to promote the orderly cross-border flow of global healthcare data.

Comparison of Regulation Models for Cross-Border Flow of Medical and Health Data

Currently, global healthcare data cross-border practices form a sample of the European Union and the United States, which represent two contrasting regulatory positions. Meanwhile, China, as an emerging market country, has a huge healthcare service market that has given rise to a huge demand for cross-border data. Including China as a research target will enhance the representativeness and scientificity of this study. As a matter of fact, the above region is the most active region in the world in cross-border regulation of healthcare data and has introduced a number of regulatory laws and regulations. Therefore, this paper focuses on analyzing the cross-border legal texts on medical data and related cases in the above regions in the past decade, and discusses the shortcomings of the current regulatory model.

EU Regulatory Framework

The EU's General Data Protection Regulation (GDPR) has been the world's most stringent regulatory act for the cross-border flow of personal data since the time of its official enactment, and a model for countries to follow. Its regulatory rules on cross-border flow of healthcare data are as follows. First, the exemption rules for authorization of cross-border flows established in Article 45 of the GDPR, ie, the principle of adequacy, which constitutes the core of the regulatory thinking of the GDPR. The Court of Justice of the European Union (CJEU), in the Schrems II CJEU decision, interpreted Articles 46(1) and 46(2)(c) of the GDPR to mean that data subjects whose personal data are transferred to a third country benefit from a level of protection essentially equivalent to the level of protection guaranteed by the GDPR and the EU Charter of Fundamental Rights. This principle requires that the third country or national organization meets the same rules for the cross-border protection of personal data as the EU itself, otherwise the data exit should be subject to a special review procedure. However, the EU currently recognizes only a few countries as meeting the adequacy standard, which does not include the United States except for commercial organizations, China.

Second, the GDPR's special exemption rules are the public interest provisions of Articles 48 and 49. Article 48 recognizes that "transfers or disclosures of personal data may be made without the authorization of European Union law on the basis of an international treaty in force" in order to achieve the international public interest, while Article 50 breaks down the circumstances in which international cooperation to promote the protection of personal data may take place. Article 49 includes "explicit consent" and "public interest" as grounds for exemption from data exit liability. Unfortunately, however, the Article does not provide clear criteria for public interest, and may face the risk of being unenforceable.

Third, Article 4 of the GDPR analyzes the concept of "genetic data", "biometric data", and "health-related data", but the criteria for classifying data are unclear. This poses a problem for healthcare providers and is a major obstacle to data sharing. Legislators should complement the GDPR rules on the cross-border issue of healthcare data and promote the enforceability of the regulation.[31]

Regulatory Model in the United States

In the US legal tradition, personal medical and health data have been protected through privacy laws, and the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, allows researchers to make reasonable use of citizens' medical and health information, which provides the possibility of cross-border transfer of medical and health data for research purposes. However, with the changes in the global data protection landscape, the US rules for cross-border transfers of healthcare data have evolved in recent years, showing a clear "two-sided" nature.

On the one hand, the US takes a liberal stance on data entry, advocating the absorption of global information and data through trade liberalization. For example, the US has pushed for the development of the Cross-Border Privacy Rules Regime (CBPR) and the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), both of which advocate for the promotion of the continued free flow of personal information across borders, in order to promote the accountability of corporate self-regulation for the protection of private information. In addition, the Clarification of Lawful Overseas Uses of Data Act of 2018 (CLOUD Act) requires all providers of electronic communications services or remote computing services within or outside the US to comply with this provision with respect to any records or other information that they maintain, or back up. This essentially adopts a long-arm jurisdictional strategy that excludes regulatory restrictions by the government of the country from which the data originated.

On the other hand, on the issue of data exit, the US has established institutional norms for foreign investment agreements with respect to data exit review through the Foreign Investment and National Security Act of 2007 (FINSA) and the Foreign Investment Risk Assessment Modernization Act of 2018 (FIRRMA). 2024 President Biden signed into law in February 2024 14,117, "Regarding the Blocking of Access by Countries of Concern to In February 2024, President Biden signed Executive Order 14117", "Executive Order on Blocking Access by Countries of Concern to Large-Scale Sensitive Personal Data of the United States and Data Relating to the Government of the United States", which restricts US companies or citizens from transmitting sensitive personal health data to certain countries, such as China, Russia, North Korea, Cuba, and Venezuela, through investments, vendor employment relationships, and other

means. In October 2024, the US Department of Justice published the Proposed Rule to Address National Security Risks to Sensitive US Data (the "Proposed Rule"), which is intended to fill a gap in the US government's authority to respond to the threat of access to sensitive US data by countries of concern. As a result, the US has taken a more nationalistic stance on data export.

Regulatory Rules in China

China's earliest legal rules on cross-border personal data were embodied in the Cybersecurity Law enacted in 2016. This law, together with the Data Security Law published in 2021, emphasizes data localization by making the value of data security the highest guideline for data transfers. In addition, Chapter 3 of the Personal Information Protection Law focuses on standards for cross-border provision of information by personal information processors, notification obligations for personal information processors, security assessment procedures for critical infrastructure operators and specific personal information processors, and reciprocal retaliatory measures for discriminatory practices in personal information protection outside of the country under Article 43. Overall, these laws take a more restrictive policy stance, prioritizing the value of security over the value of mobility.

Beyond the law, China has established the State Internet Information Office (CAC) as the administrative authority for cross-border data flows. Specific implementation measures have been introduced. The department issued the Measures on Data Exit Security Assessment in 2022, which stipulates that data processors should apply for data exit security assessment, assessment matters, application materials, types of risks, standard contracts, as well as hearing procedures and deadlines, etc. The Provisions on Promoting and Regulating Cross-border Flow of Data, which came into force in 2024, further clarifies the obligation of data processors to declare important data, establishing the three systems: data exit security assessment, standard contract for personal information exit, and personal information protection certification. This provision relaxes the conditions for cross-border flow of data and narrows the scope of data outbound security assessment. According to CAC data, the average number of monthly declarations for data exit security assessment has dropped from 13 before the introduction of the Provisions to 5 at present, a decrease of 60%; the average number of monthly filings for standard contracts for the exit of personal information has dropped from 72 to 37, a decrease of 48%; and the average time for security assessment has dropped to less than 30 working days.[32]

Until now, China has not yet issued legal documents specifically addressing the cross-border flow of healthcare data. However, China has delegated the discretionary power to review healthcare data outbound to free trade zones or free trade port administrations across the country. These administrations have developed their own negative lists for the categorization and classification of healthcare data, taking into account their actual needs and based on laws and regulations. The advantage of the negative list system is that it follows the private law concept of prioritizing freedom and reduces the access risk and innovation risk of healthcare data processing subjects.

Deficiencies of the Three Regulatory Frameworks

Differences in Regulatory Concepts

Data security is a further extension of Hobbesian natural law ideas in contemporary society, and its derivation of data statism or data localizationism has begun to rise globally. The EU advocates data sovereignty on the grounds of personal data rights protection. This is related to its right to personal data being recognized as a fundamental right by the EU Charter of Fundamental Rights, making the EU data protection framework embedded with non-economic objectives.[33] The US, on the other hand, has demonstrated a strong stance on the free inflow of data and outflow restrictions based on national security, a nationalism that is mixed with ideological factors and reflects the pursuit of maximizing US data interests. China, on the other hand, has long insisted on data sovereignty on the grounds of national data security, but in 2024 it relaxed its ex ante regulatory efforts, emphasizing instead the whole chain of ex ante, mid and ex post regulation.[34] This means that China is shifting to more relaxed rules for cross-border flow of healthcare data, advocating a free-flow-of-information model with strong potential economic incentives to do so.[35]

Clearly, the three typical approaches described above reveal different national interest orientations. Among them, the US and some countries in the EU advocate the absorption of global data development benefits and take a passive stance on policies that promote international interests and human rights. Such philosophical differences are exacerbating data

trade frictions and disputes between countries, and as the right-winging tendency of global politics becomes more pronounced, healthcare data will face more obstacles across borders. In addition, data suggests that about 58% of the loss of EU data exports comes from an increase in its own restrictions, rather than from the policy behavior of its partners.[36] These policy barriers will not only jeopardize the investment interests of enterprises, but also reduce the smoothness of cooperation in the field of biomedicine and ultimately affect the healthcare welfare of at least 2.2 billion people in the three regions.

Non-Consistency in the Connotation of Data Regulatory Rules

At the rule level, national legislators have adopted legal schemes with wide variations. For example, Article 49(1)(d) of the EU GDPR sets out "the transfer is necessary to achieve the public interest" as a derogation rule for healthcare data rights, but states that the "public interest" should be recognized by EU or Member State law. This is an enabling provision that allows the EU or its Member State authorities to determine and apply it at their own discretion, and is therefore a legal concept of uncertainty. In CE-No. 444937, the French Conseil d'Etat held that it was in the public interest to allow the use of health data in the context of the Covid-19 crisis, and accordingly held that it was in the public interest for Microsoft to authorize the US public authorities to access personal information collected by them. As can be seen, a case-by-case judgmental path may have to be taken regarding the recognition of public interest. In China, Article 3 of the Provisions on the Promotion and Regulation of Cross-border Flow of Data lists academic cooperation as an exemption from data exit, but the provision does not clarify the relationship between the values of security and freedom upheld by the supreme law, so the standard of review is unclear. As for the US data exit regulation policy, especially the restriction policy on specific countries, it also faces the flaws of unconvincing national security reasons and vague restriction circumstances.

In addition, the healthcare data exit scenario is a hierarchical and categorized control of healthcare data in terms of security, privacy, and other dimensions. By clarifying the prohibitions or restrictions on data exit, it can better guide the cross-border compliance behavior of individuals or enterprises with healthcare data. However, not all countries or regions have clear or consistent healthcare data exit scenarios. For example, the GDPR categorizes healthcare data into three concepts: "genetic data", "biometric data" and "health-related data". However, it is questionable whether "health-related data" includes genetic data and biometric information, the latter two of which are often inextricably linked to healthcare activities. China differs from the above approach by specifically proposing security assessment scenarios for the exit of personal data, including two categories of entities, namely, critical information infrastructure operators and other data processors, and three categories of data, namely, important data, personal information (excluding sensitive personal information), and sensitive personal information. The US applies privacy rules to regulate the export of personal medical and health data, forming a dual regulation model of "personal sensitive information + personal privacy", which can be subdivided into "human genome data", "personal health data", "personal data", "personal data" and "personal data". The former can also be subdivided into "human genome data", "personal health data" and "personal sensitive data".

The above legal concepts are ambiguous, resulting in a large room for discretion in healthcare data exit scenarios. As a result, such a discrepant policy may restrict healthcare trade and technology cooperation between the two sides, firstly making healthcare service providers face the cost of building a compliance system, and also bear the result of being penalized by the authorities. At the same time, pharmaceutical researchers may thus be prevented from accessing the obstacles of adequate experimental data and patient feedback, seriously affecting the availability of biopharmaceutical R&D and medical technology advances.[37] Finally, it also prevents the effect of medical and health information sharing among countries and between countries and international organizations.

Lack of Cooperation and Governance at Different Levels

The multiple values attached to medical and healthcare data, such as security interests and property gains, make the regulation of cross-border data flow no longer simply fall into the category of administrative control, but rather a matter of public-private law, thus generating the need for governance that takes into account multiple legal values in a comprehensive manner. At this stage, the regulatory body of cross-border flow of medical data is still administratively dominated, and the participation of enterprises, individuals and even non-governmental organizations and industry

associations is insufficient, which restricts the effectiveness of cross-border regulation of data in a certain procedure. In addition, the divergent interests of countries have led to the fact that an effective governance mechanism has not yet been formed at the international level, which will make the cross-border regulation of medical data remain in a state of fragmented regulation.

Overall, however, determining the relationship between appropriate legal restrictions and the free flow of cross-border data is a difficult task, and highly regulatory regimes are not necessarily effective.[38] Moreover, the logic of data security policies still varies from country to country, with political factors gradually becoming dominant, which is not conducive to realizing the legal value of healthcare data. Therefore, how to go beyond the existing regulatory frameworks and rules to build regulatory rules for the cross-border flow of healthcare data that reflect the "consensus on fundamental human rights" is a fundamental issue to be resolved. In fact, the international right to health care is the key to this issue.

A Human Rights Perspective on the Regulation of Cross-Border Flows of Healthcare Data

Medical and health data possess significant public welfare implications, and a regulation model focused primarily on restrictions and prohibitions can hinder the advancement of global public health security. From a rights-based perspective, the regulation of cross-border medical and health data may conflict with citizens' entitlements to health rights. This section analyzes the legal foundations of cross-border medical and health data from the viewpoint of international human rights, examines the obligations of states regarding medical and health rights, and explores the tensions between these rights and the regulation of cross-border data flow.

The Right to Medical Health and Its State Obligations

The moral basis of the right is life, and life is the form in which a human being can live in good health. As a whole, the right to health is closely related to the right to development, since the ultimate meaning of human development is the existence of human life.[39] Both the right to health provisions in the constitutional framework of the United Nations and the regional conventions on the protection of rights, represented by the European Charter of Rights, recognize the level of health care as a necessary condition for the promotion of human health and the maintenance of life. Article 25 (1) of the Universal Declaration of Human Rights includes as part of the right to an adequate standard of living "the right of everyone to a standard of living adequate for the health and well-being of himself and of his family", and Article 12 of the Covenant on Economic, Social and Cultural Rights systematically clarifies the content of the right to health by stating that "everyone has the right to the enjoyment of the highest attainable standard of health". Article 12 of the Covenant on Economic, Social and Cultural Rights systematically clarifies the content of the right to health, stating that "everyone has the right to the enjoyment of the highest attainable standard of physical and mental health", expanding the content of the right to health to include basic health-care services and other prerequisites, the latter of which include basic elements such as the human environment, food and water and air quality.

The right to health is similar to the right to life in that it is inherent in all human beings and implies not only the negative aspect of freedom, which excludes outside interference, but also the positive aspect of the need for the State to actively safeguard it. The right to health care, on the other hand, implies not only the right not to be subjected to unlawful interference in treatment, but also the ability to provide at least a sufficient amount of health care services. The right to health is a law-based right that can be realized through a complex legal framework of constitutional, civil and administrative law.[40]

Based on the theory of State duty of fundamental rights, States should fulfill their duties at three levels: to respect, to protect and to give. At the level of the obligation to respect, the State should prohibit acts that unlawfully harm health or interfere with medical practices, and the State itself should prohibit its agencies and staff from accessing personal medical and health information when it is not necessary to do so. In terms of the duty to protect, the state should take the initiative and provide adequate procedural and remedial mechanisms to protect citizens from infringement of their health information. As for the State's obligation to pay, the State is required to provide effective healthcare resources within the State's capacity, including professional personnel, institutional space, medicines and equipment, free public services,

scientific research, international cooperation, and so on. Indeed, as the right to health care is a common moral obligation or duty towards others, the obligation to provide health care must be provided in a non-discriminatory manner so that the right has the potential for universal realization.[41,42]

As a fundamental right, the right to health refers to essential healthcare services, which are of considerable importance and require States to improve the internal and external resilience of their public health systems, especially if a country is lagging behind in terms of overall healthcare standards or is technologically weak in specific areas of healthcare. In other words, since the right to health has been recognized by the international community as a fundamental right to be protected, States parties have not only an obligation to provide international cooperation and assistance in the field of health care, but also a specific obligation to promote the implementation of their national legislation and enforcement of guarantees.

Data Protection and Regulation of Cross-Border Data Flows in the Framework of Human Rights

In the field of healthcare, it is the uneven distribution of medical resources and technologies worldwide that has led to the rapid development of medical production, medical research and trade in biomedicine. In response to the gap between economic and social and national scientific and technological levels, cross-border medical and scientific research cooperation will be an important way to enhance the public health capacity of disadvantaged countries, which is also the result of the fulfillment of the state's obligations under international law and domestic protection obligations. Indeed, cross-border health data sharing is essential to facilitate important health research into new treatments and to improve patient care and safety.[43] This is because sharing data will increase confidence and trust in the conclusions of clinical trials and help achieve independent confirmation (reproducibility) of results.[44] The COVID-19 pandemic has demonstrated the value of sharing health data across countries for collaborative operational and research purposes, and in particular has led to the important achievement of developing highly effective vaccines at an unprecedented rate.[45] China's Beijing Municipal Internet Information Office approved an application for medical data exit in June 2023 for a collaborative research project between Beijing Friendship Hospital of Capital Medical University and the University of Amsterdam Medical Center in the Netherlands, which became the first approved case of data exit security assessment (No. 20220001) in China. This case fully illustrates the necessity of cross-border flow of medical data.[46]

In fact, from the perspective of global public interest, medical and health data are widely used for disease treatment, physical health care, and health prevention and treatment, and can be treated as a public good.[47] For example, for common diseases, adequate data flow and sharing will enhance medical treatment and drug development. One report shows that patient data sharing can increase the number of clinical trials by about 14% compared to a situation where there is no patient data sharing. In the case of oncology trials, for example, the success of these trials could potentially lead to 64,000 quality-adjusted life years for cancer patients in the EU. Conversely, hindering current progress in data sharing could add around €5.4 billion in costs between the EU and non-EU regions, which is equivalent to around 50% of the current value of such data streams.[48] For rare diseases (RD), identifying and collecting sufficient data individually will be made more difficult by the fact that patient populations are small in many countries/regions.[49] Meanwhile, research on RD is dispersed in laboratories and clinics around the world, and this paucity of expertise and practice translates into diagnostic delays, scarcity of medicines, and difficulty in accessing care.[50] Therefore, we need an adequate policy environment for cross-border data.

The results of a 2022 survey study showed that 80% of respondents reported having accessed care via telemedicine at some point in their lives, an 8% increase from 72% in 2021; especially among chronically underserved groups in healthcare, such as 55+ year olds, and respondents living in rural areas, who have seen a significant increase in telemedicine utilization.[51] Therefore, instead of excessively restricting the cross-border flow of healthcare data, sovereign states should guarantee the right of residents to enjoy cross-border healthcare services, promote cross-border medical cooperation, and develop cross-border pharmaceutical industries. However, the value requirement of human rights itself constitutes a violation of state sovereignty, as states cannot regulate or violate internationally binding laws.[52] Therefore,

the cross-border demand for data arising from the above links requires government authorities to optimize regulatory policies and exercise prudence.

Unfortunately, however, this is not fully recognized by States. The current increasingly stringent regulatory rules for cross-border flow of data globally are unhelpful to the guarantee of the right to health and medical care. To some extent, the new wave of global data legislation modeled on the GDPR may simply be an "unconscious group" following suit, with each country not knowing exactly why it is prohibiting or restricting cross-border data flows. Therefore, the primary value of regulating cross-border data flows should be the promotion of international human rights, rather than national interests and the economic value of data flows.

Model Unfolding for Human Rights Regulation of Cross-Border Flows of Healthcare Data

The cross-border flow of medical data should take into account the balanced relationship between international human rights, national security, and the value of rights, so as to realize the stability of the "value triangle" of cross-border regulation of medical and health data. The increase in the number of international public health emergencies (PHEICs), represented by COVID-19, shows the divergent and fragmented attitudes of countries in their governance positions and policies, which has led to differences in the traceability of viruses, criteria for recognizing illnesses, and methods of treatment by medical institutions, resulting in the spread of these outbreaks globally, and further disadvantaging lagging regions as well as disadvantaged groups. This bitter lesson requires the strengthening of international cooperation in the field of public health.

Promoting Cooperative Governance Through International Human Rights Cooperation Mechanisms

Policymakers around the world have embraced the concept of health data as an "asset" to ensure economic growth through biomedical research and innovation.[53] However, crossing borders with healthcare data is not an easy task, and increasing data nationalism will continue to exacerbate the regulatory environment for cross-border data. There are significant gaps in the existing international legal framework, which are inadequate to deal with the complexities and nuances of the digital age.[54] In the context of the Internet, where data can be easily and rapidly moved across borders, cross-border data flows present a more complex clash of privacy cultures.[55] Promoting consistency or convergence of privacy protection rules is a prerequisite for enhancing trust in digital human rights. According to this logic, States should exercise great restraint in regulating cross-border data flows, and national information policies may need to be formulated in a way that takes into account communication, business and economic management concerns.[10] Based on this, the international community should reach a basic consensus on data crossing borders and seek a minimum ethical basis, which is precisely the basis of legitimacy for transnational research and service expansion in healthcare.

The Global Digital Compact (GDC), adopted in 2024, states in its purpose: "In order to achieve our goals, we will strive to 1. bridge all digital divides and accelerate the achievement of the Sustainable Development Goals (SDGs); 2. broaden the inclusiveness of the digital economy so that all people can benefit from it; and 3. create an inclusive, open, safe and secure digital space that respects, protects and promotes human rights; 4. advancing responsible, fair and interoperable approaches to data management; and 5. strengthening international governance of artificial intelligence for the benefit of humanity". The Compact has three core concepts, namely human rights, development, and governance.[56] This is an important way of thinking about addressing existing inequalities in healthcare or obstacles to the full realization of sustainable development.

Therefore, the first task for policymakers in all countries is to actively promote the UN-centered data human rights governance rules, clarify the framework of rules for cross-border flow of healthcare data in the form of an international convention, and set up a specialized agency to oversee the regulatory conduct of cross-border flow of data. At the same time, there is a need to enhance the policy promotion function of the World Organization for Human Rights and the World Health Organization, and to realize the potential of the International Health Regulations. Of course, the above organizations should also promote the development of international conventions for cross-border cooperation on

healthcare data to strengthen global health security and reduce the huge economic losses caused by global health emergencies.[57]

Second, facilitating cross-border flow of data should also promote consistency in technical rules for data systems. Because the lack of interoperability in most healthcare systems results in a lack of data mobility, about one-third (38%) of countries do not have clinical standards or vendor certification for EHR systems, which limits the interoperability of health data.[58] On a positive note, adequate cross-border policies for healthcare data will facilitate cross-border personalized medical diagnostic services and promote pharmaceutical and medical device companies to improve the safety and efficacy of their products. Therefore, countries should promote the consistency of healthcare data system infrastructure to enhance the convenience of cross-border flow.

In addition, cooperation on healthcare data rights remedies should be strengthened. Artificial intelligence has been deeply applied in a wider range of data domains, and some online service operators use intelligent algorithms to characterize the public image and push commercial advertisements to specific groups. Such behavior may involve unlawful infringement of personal rights and interests, including privacy, and the main sanction is administrative punishment or judicial adjudication of the offending subject, but it faces the obstacles of transnational evidence collection and judicial collaboration. In the context of cross-border data flows, individuals may not be able to access their own records in foreign countries.[59] Taking cross-border data transactions as an example, consumers can only obtain remedies through relevant contracts and domestic laws, and there is a lack of transnational online consumer protection mechanisms and remedies,[60] which is one of the reasons why the legislation of various countries tends to restrict cross-border data flows. Therefore, countries should continue to promote the cooperation mechanism of medical and health data damage relief system under the premise of unified regulatory rules for cross-border data flow and multilateral agreements, and promote synergies in matters such as investigation and evidence collection and judicial assistance.

Promoting Regulatory Mutual Recognition Mechanism by Way of Economic and Trade Cooperation

In order to promote the free flow of data across borders in an orderly manner, the data regulatory rules and Internet regulations formulated by the countries concerned should have the possibility of interoperability, and ensure mutual recognition of the standards or criteria for authorization, licensing or certification among them. However, in the absence of an international convention on the cross-border flow of healthcare data, there is a need for more international harmonization of domestic regulations on the licensing, certification or authorization of service providers. An effective way of doing so is to promote consistency of national regulatory policies through various economic and trade rules.

Under the WTO framework, the Marrakesh Agreement Establishing the World Trade Organization (GATS) requires members to have general obligations and specific commitments on market access and national treatment. Its specific commitments require each member to designate basic terms, restrictions, conditions and time frames applicable to the industry as a whole. However, the WTO mechanism was formed at a time when Internet technology was far less developed than it is today, and thus there were no special provisions for cross-border flow of data. However, the new generation of free trade agreements acts as a complement to the WTO regime, which makes WTO law and case law relevant in assessing the legality of regulations on cross-border data flows under the new instrument.[61] Therefore, countries can advance the negotiation of restrictions on cross-border data flows under the WTO mechanism, and agree on basic healthcare data regulation rules based on the public interest provisions of GATS to facilitate the efficient flow of data activities.

In addition, parties can independently carry out bilateral and multilateral negotiations on cross-border flow of data, or promote cross-border flow of healthcare data by signing free trade agreements.[62] The main agreements on healthcare data cross-border include the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the Digital Economy Partnership Agreement (DEPA), the Regional Comprehensive Economic Partnership Agreement (RCEP), the U.S.-Mexico-Canada Trade Agreement (USMCA), the EU-US Data Privacy Framework (DPF), the Atlantic Declaration: the 21st Century U.S.-UK Economic Partnership Framework (ADAPT), etc. These FTAs generally advocate the free flow of data, tend to be conservative in their approach to data-restrictive regulation, and increasingly share the same regulatory

standards. Among them, RCEP has constructed a paradigm for cross-border data flows in Asia that matches the development status of Asia-Pacific countries, which is worthy of emulation by other developing countries.[63] In addition, China and the EU established the China-EU Cross-Border Data Flow Exchange Mechanism at the national level in 2024 to promote the construction of regulatory frameworks in the form of meetings. There have been frank, in-depth and constructive exchanges.

These practices imply the importance of promoting the establishment of mutually beneficial institutional arrangements through economic and trade cooperation. Therefore, countries also need to recognize each other's eligibility requirements and procedures, technical standards and licensing requirements for data flows, etc., to enhance interoperability. In addition, governments should build an information management platform for healthcare data exit, enhance international data exit information sharing, respond to the reasonable concerns of all parties, and strengthen mutual trust.[64]

Improving the Data Interest Protection Mechanism for Underdeveloped Countries

In their efforts to bridge the global digital divide, countries seek to attract and engage foreign investors to help develop their digital prowess in areas such as infrastructure, Internet services and digital solution providers.[65] That is, countries or regions that use data security as the purpose of cross-border regulation of healthcare data have a policy goal of enabling the development of their data industries. This is because this type of model requires data to be stored locally and prohibits or restricts data cross-border behavior as appropriate. For example, the European Union and the United States negotiated the Data Privacy Framework with the aim of localizing soft data and restricting the market competitiveness of foreign technology firms within its borders, to provide data and technology safeguards for the implementation of its technology sovereignty strategy.[66] The United States, on the other hand, interferes with the data sovereignty of developing countries, squeezes the data policy space of developing countries, and pushes developing countries to accept unequal data rules and other external contradictions by dominating the rules of regional economic agreements such as APEC.[67]

The promotion of digital sovereignty and the right to digital development of developing countries is a basic moral requirement of international data governance and an inevitable consideration of data human rights governance. Only in this way can we guarantee the participation of equal developing countries in the process of digital globalization and realize the digital rights and interests of their nationals. However, the relationship between the cross-border flow of healthcare data and the realization of the right to digital development of developing countries is quite complicated, and developing countries need to face the unfairness of the global regulatory rules on the cross-border flow of healthcare data. To this end, the adjudication rules for cross-border services and trade in healthcare data should be improved, the necessity and reasonableness of cross-border data restriction measures should be investigated, arbitrary and discriminatory policies should be prohibited, and the interests of disadvantaged countries should be safeguarded. Second, data governance assistance from developed countries or the international community to developing countries should be promoted with reference to relevant international assistance practices. For example, the international community should take into account the specific circumstances of developing countries and LDCs that are lagging behind in data use and management, and require developed countries to mandatorily assist developing countries and LDCs in developing their data regulatory infrastructure, creating an interoperable framework for health data sharing, and carrying out the cross-border flow of health and genomic data on the basis of clear rights and responsibilities and in an ethical manner, so as to improve the level of medical and health protection in developing countries. (d) Establishing a coordinated participation of multiple actors.

Establishing a Regulatory Framework with the Collaborative Participation of Multiple Actors

Individuals or enterprises are often able to collect and process personal data by virtue of their technological advantages, and become important providers of data products. It is also because of their technical and professional advantages that various large-scale data platform companies in fact share the right to participate and even the right to make decisions on data governance and rule-making. The Internet governance system is multi-stakeholder in nature, and most privacy and security issues related to digital technology need to take into account the central role of market players in ensuring the openness and security of data flows and realizing the self-regulation of such players in the field of high technology.[68]

This is because data platform companies act on the economic value of data and pursue data revenue maximization, giving them a certain degree of initiative in data cross-border rulemaking or rule articulation. The high sensitivity of healthcare data, the difficulty of distinguishing between types, and the uncertainty of security risks require large entities such as important multinationals and major data processors to assume responsibility for self-governance. For example, they should set up special legal compliance departments to strengthen the construction of data exit compliance systems, formulate early warning programs for regulatory failures according to their own special needs, and improve their organizational capacity to deal with all kinds of potential risks and emergencies in data cross-border. At the same time, enterprises should establish complete rules for the collection and processing of personal data and privacy, and restrict their business behaviors in accordance with the competition law and personal information protection law, so as to reduce the risk of violation of the law. Of course, it is even more important that cross-border data regulators should strengthen communication with platform companies to formulate acceptable and feasible rules and programs.

Meanwhile, the lobbying function of healthcare and data industry associations should also be utilized. Modern society is a network of relationships woven together by relying on various relationships, which in turn form specific interest groups. Based on the refinement and redundancy of risk-based administration, limited administrative resources are unable to comprehensively regulate all aspects of social behavior, and it is inevitable to seek an articulated entity between the market and the state, thus contributing to a pattern of shared governance. With the expansion of medical, healthcare and medical research cooperation, and the complexity of public health governance, there is a great need for industry associations in the healthcare sector. These organizations, with their professional strengths, can promote standardization in these areas and enhance the consistency of self-action. However, it is difficult to find the role of industry associations, let alone other non-governmental organizations, whether from the EU GDPR, or China's data cross-border regulatory rules, or other countries' data cross-border governance models. Therefore, it is important to promote third-party governance in the field of healthcare data and to utilize the technical standard power of healthcare industry associations. Encourage them to participate in legislative proposals, policy formulation and standard-setting activities through research reports, professional conferences, etc., to enhance the compliance of healthcare data outbound entities.

Conclusion

Cross-border data regulation is a vast and new area of work, and healthcare data cross-border faces even greater challenges. However, the balance between technological advancement and economic growth, protection of individual privacy and national security has become the "triple dilemma" of healthcare data cross-border regulation. Currently, major economies such as the US, China and the European Union (EU) have adopted different strategies for strong cross-border regulation of healthcare data, resulting in serious obstacles to global healthcare data sharing. However, the core of this debate does not lie solely in the combination of the values of freedom, rights and security, but rather in the concept of international human rights in relation to healthcare, which should be the basis for national policies.

Indeed, a global consensus should be reached on the ontology of healthcare data and, on the basis of supporting appropriate restrictions on the cross-border flow of healthcare data, prudent data localization measures should be taken, transparency in cross-border regulation of data should be improved, and the rights and interests of vulnerable countries in relation to healthcare data should be protected. Therefore, countries should promote the consistency of technical rules for data systems and enhance cooperation on healthcare data rights remedies through UN Charter mechanisms and human rights governance mechanisms. Second, the convergence of regulatory rules should also be promoted through the WTO framework and free trade agreements, etc., to reach consensus on general rules, public interest provisions, and liability mechanisms. Of course, both the human rights governance strategy and the accompanying economic and trade governance programs must take the realization of the data rights and interests of developing countries as a target guideline to achieve distributive justice in the global healthcare data benefits. On this basis, the free cross-border flow of healthcare data under the overall human rights perspective is emphasized, and the effectiveness of governance is enhanced through the self-regulation of healthcare data cross-border entities.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Metille S. Swiss information privacy law and the transborder flow of personal data. *J Int Commercial Law and Technol*. 2013;1:71–80.
2. Nguyen D, Paczos M. *Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective. OECD Digital Economy Papers*. Vol. 297. Paris: OECD Publishing; 2020. doi:10.1787/6345995e-en
3. Maugeri A, Barchitta M, Basile G, Agodi A. A public and research interest in telemedicine from 2017 to 2022: infodemiology study of google trends data and bibliometric analysis of scientific literature. *J Med Internet Res*. 2024;26:e50088. DOI:10.2196/50088
4. How to harness the power of health data to improve patient outcomes, Avialable from: https://www.weforum.org/stories/2024/01/how-to-harness-health-data-to-improve-patient-outcomes-wef24/. 2024. Accessed December 19, 2024.
5. LeSieur F. Regulating Cross-Border Data Flows and Privacy in the Networked Digital Environment and Global Knowledge Economy. *Int Data Privacy Law*. 2012;2(2):93–104. doi:10.1093/idpl/ips004
6. Chaisse J. 'The Black Pit:' power and pitfalls of digital FDI and cross-border data flows. *World Trade Review*. 2023;22(1):73–89. doi:10.1017/S1474745622000337
7. Beling CT. Transborder data flows: international privacy protection and the free flow of information. *Boston Coll Int Comparative Law Rev*. 1983;6(2):591–624.
8. Dorine RS. Transborder data flow: regulation of international information flow and the Brazilian Example. *J Law Technol*. 1986;1(1):31–66.
9. Jane AZ. Transborder data flow: problems with the council of Europe convention, or protecting states from protectionism. *Northwestern J Int Law & Business*. 1982;2(4):601–625.
10. Wellington Brown R. Economic and trade related aspects of transborde r data flow: elements of a code for transnational commerce. *Northwestern J Int Law & Business*. 1984;6(1):1–85.
11. Hardy IT Jr. Transborder data flow: an overview and critique of recent concerns. *Rutgers Computer & Technology Law Journal*. 1983;9(2):247–264.
12. Han X. Paradigm Shift of European Union (EU) in cross-border data flow supervision-from the perspective of digital services legislation. *J WTO and China*. 2023;13(2):69–94.
13. Dutch SA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US, Available from: https://www.edpb.europa.eu/news/news/2024/dutch-sa-imposes-fine-290-million-euro-uber-because-transfers-drivers-data-us_en. Accessed December 4th, 2024.
14. Gregory Voss W. Cross-border data flows, the GDPR, and data governance. *Washington Int Law J*. 2020;29(3):485–532.
15. Clarifying the legal requirement for cross-border sharing of health data in POPIA: recommendations on the draft Code of Conduct for Research. *South Afr J Bioethics Law*. 2024;17(1):e1696. doi:10.7196/sajbl.2024.v17i1.1969
16. Chen Y, Song L. China: concurring regulation of cross-border genomic data sharing for statist control and individual protection. *Hum Genet*. 2018;137(8):605–615. doi:10.1007/s00439-018-1903-2
17. Grossman GS. Transborder data flow: separating the privacy interests of individuals and corporations. *Northwestern J Int Law & Business*. 1982;1(4):1–36.
18. Chin Y-C, Zhao J. Governing cross-border data flows: international trade agreements and their limits. *Laws*. 2022;11(4):1–22. doi:10.3390/laws11040063
19. Aaronson S. Why trade agreements are not setting information free: the lost history and reinvigorated debate over cross-border data flows, human rights, and national security. *World Trade Review*. 2015;14(4):671–700. doi:10.1017/S1474745615000014
20. Pan D, Hao Y, Qiao P, et al. Research on risk categorization and supervision strategy of cross-border data flow. *Manage Rev*. 2024;07(36):43–53.
21. Bradford L, Aboy M, Liddell K. Standard contractual clauses for cross-border transfer of health data after schrems II. *J Law Biosci*. 2021;1(8):1–36.
22. Becker R, Chokoshvili D, Dove ES. Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing? *Int Data Privacy Law*. 2024;14(3):223–246. doi:10.1093/idpl/ipae014
23. Minssen T, Seitz C, Aboy M, Corrales Compagnucci M. The EU-US privacy shield regime for cross-border transfers of personal data under the gdpr: what are the legal challenges and how might these affect cloud-based technologies. big data, and ai in the medical sector? *Eur Pharm Law Rev*. 2020;1(4):34–50. doi:10.21552/eplr/2020/1/6
24. Liverani M, Teng S, Le MS, et al. Sharing public health data and information across borders: lessons from Southeast Asia. *Global Health*. 2018;14(94). doi:10.1186/s12992-018-0415-0
25. Tamuhla T, Lulamba ET, Mutemaringa T, Tiffin N. Nicki Tiffin - Multiple modes of data sharing can facilitate secondary use of sensitive health data for research. *BMJ Global Health*. 2023;8(10):e013092. doi:10.1136/bmjgh-2023-013092
26. Clark S, Weale A (2011) Information governance in health. Research report. University College London.
27. Price WN, Cohen IG. Privacy in the age of medical big data. *Nat Med*. 2019;25(1):37–43. doi:10.1038/s41591-018-0272-7
28. Reichel J. Oversight of EU medical data transfers – an administrative law perspective on cross-border biomedical research administration. *Health Technol*. 2017;7(4):389–400. doi:10.1007/s12553-017-0182-6
29. Svantesson DJB. The regulation of cross-border data flows. *Int Data Privacy Law*. 2011;1(3):180–198. doi:10.1093/idpl/ipr012
30. Health data breach: Dedalus Biologie fined 1.5 million euros, Available from: https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en. Accessed December 4, 2024.
31. Jones E. The GDPR Two Years on. *Antitrust*. 2020;35(1):51–57.
32. Yang J. "State Net Information Office: the expected goal of promoting cross-border flow of data is basically realized". Available from: http://jnzstatic.cs.com.cn/zzb/htmlInfo/df02b49b901a46ce9689c0809ed002e8.html. Accessed December 4, 2024.
33. Yakovleva S. Personal data transfers in international trade and eu law: a tale of two 'necessities'". *J World Invest Trade*. 2020;21(6):881–919. doi:10.1163/22119000-12340189
34. Liu J. Application and improvement of personal information exit regulatory exemption system under the dual-track system of cross-border data. *Finance and Economics Law*. 2024;05:23–40.
35. Guo S, Xiang L. Cross-border data flow in China: shifting from restriction to relaxation? *Comput Law Secur Rev*. 2025;56:106079. ISSN 0267-3649.doi:10.1016/j.clsr.2024.106079
36. Frontiers Economics. *The Value of Cross-Border Data Flows to Europe: Risk and Opportunities*; 2021.

37. Data Alliance G, White Paper: data transfers under the EU proposal on the European health data space, Available from: https://globaldataalliance.org/sectors/healthcare/. December 4, 2024.
38. Branscomb AW. Global governance of global networks: a survey of transborder data flow in transition. *Vanderbilt Law Rev*. 1983;36(4):985–1044.
39. de Vasconcelos FA, Casas Maia M. The right to health and the right to development. *Direito e Desenvolvimento*. 2012;3(6):65–81. doi:10.26843/direitoedesenvolvimento.v3i6.210
40. Julesz M. "The Right to Health", Jura. *A Pecsi Tudomanyegyetem Allam-es Jogtudomanyi Karanak Tudomanyos Lapja 2018*. 2018; 2: 136–148.
41. Friesen T. The right to health care. *Health Law J*. 2001;9:205–222.
42. Jamar SD. The international human right to health. *Southern Univ Law Rev*. 1994;22(1):1–68.
43. Richards R. Barriers on cross-border sharing of health data for secondary use and options to overcome these. *Eur J Public Health*. 2022;32(Suppl 3):ckac129.367. PMCID: PMC9594075.doi:10.1093/eurpub/ckac129.367
44. Hulsen T. Sharing is caring-data sharing initiatives in healthcare. *Int J Environ Res Public Health*. 2020;17(9):3046. PMID: 32349396; PMCID: PMC7246891.doi:10.3390/ijerph17093046
45. HIMSS. (2023). Report. Available from https://www.himss.org/resources/empowered-cloud-how-cross-border-health-data-flows-can-create-value-patients-and-boost. Accessed December 19, 2024.
46. Beijing Friendship Hospital: Nation's first approved data exit security assessment case lands at Beijing friendship hospital, Available from: https://www.bfh.com.cn/Html/News/Articles/5797.html. accessed December 4, 2024.
47. Carter P, Laurie GT, Dixon-Woods M. The social licence for research: why care. data ran into trouble. *J Medical Ethics*. 2015;41(5):404–409. doi:10.1136/medethics-2014-102374
48. Frontiers Economics, The value of international health data flows for the EU: a report prepared for Roche, 2023.
49. Aagaard L, Kristensen K. Access to cross-border health care services for patients with rare diseases in the European Union. *Orphan Drugs: Research and Reviews*. 2014;39–45. doi:10.2147/ODRR.S58268
50. Julkowska D, Austin C, Cutillo C, et al. The importance of international collaboration for rare diseases research: a European perspective. *Gene Ther*. 2017;24(9):562–571. doi:10.1038/gt.2017.29
51. Knowles M, Krasniansky A, Nagappan A, Consumer adoption of digital health in 2022: moving at the speed of trust, Available from: https://rockhealth.com/insights/consumer-adoption-of-digital-health-in-2022-moving-at-The-speed-of-trust/. Accessed December 4, 2024.
52. Slaughter A-M. Sovereignty and power in a networked world order. *Stanford J Int Law*. 2004;40:283–327.
53. Tarkkala H, Helén I, Snell K. From health to wealth: the future of personalized medicine in the making. *Future*. 2018;109:142–152. doi:10.1016/j.futures.2018.06.004
54. Qian X. Redefining international law paradigms: charting cybersecurity, trade, and investment trajectories within global legal boundaries". *J World Invest Trade*. 2024;25(3):295–333. doi:10.1163/22119000-12340327
55. Le Sieur F. Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. *Int Data Privacy Law*. 2012;2(2 2012):93–104.
56. Zhang W. The global digital compact is a landmark achievement of digital civilization. *Law and Soc Dev*. 2024;30(06):2.
57. Gostin LO, Katz R. The international health regulations: the governing framework for global health security. *The Milbank Quarterly*. 2016;94(2):264–313. doi:10.1111/1468-0009.12186
58. OECD. *Health at a Glance 2023: OECD Indicators*. Paris: OECD Publishing; 2023. doi:10.1787/7a7afb35-en
59. Cooper DM. Transborder data flow and the protection of privacy: the harmonization of data protection law. *Fletcher Forum*. 1984;8(2):335–352.
60. McGillivray K. A right too far? Requiring cloud service providers to deliver adequate data security to consumers. *Int J Law and Inform Technol*. 2017;25(1):1–25. doi:10.1093/ijlit/eaw011
61. Rotenberg J. Privacy before Trade: assessing the WTO-consistency of privacy-based cross-border data flow restrictions. *Univ Miami Int Comparative Law Rev*. 2020;28(1):91–120.
62. Dayday CMGT. Cross-border data flows and data regulation under international trade law. *Philippine Law J*. 2023;96(1):33–81.
63. Zhai D. RCEP Rules on Cross-Border Data Flows: asian characteristics and implications for developing countries. *Asia Pacific Law Rev*. 2024;1–22. doi:10.1080/10192557.2024.2417949
64. He J, Zhang X. Exploring the regulation of cross-border flow of healthcare data in China. *Int Law Res*. 2022;06:62–74.
65. Chaisse J, Bauer C. Cybersecurity and the protection of digital assets: assessing the role of international investment law and arbitration, 21. *Vanderbilt J Entertainment and Technol Law*. 2020;21:549.
66. Liu Y. The EU's technology sovereignty strategy and its realization in the US-EU data cross-border flow game. *Int Law Res*. 2023;(06):64–85.
67. Yanhua L. Digital development rights in developing countries: where the governance rules for cross-border data flows. *J Human Rights*. 2023;22(5):1040–1066.
68. Shackelford SJ, Raymond A, Charoen D, et al. When toasters attack: a polycentric approach to enhancing the security of things. *Univ Illinois Law Rev*. 2017;439.