PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 1 February 2025

# Emerging Challenges of Smart Wearable Devices: Enhancing Personal Health Information Protection in China

**Yuxin Ji[1], Yumeng He[1], Xiaoyi Li[1], Baili Yi[1], Qinghua Han[1] & Yun Chen[1]**

[1] School of Law, Tianjin Normal University, Tianjin, China
Correspondence: Yumeng He, School of Law, Tianjin Normal University, Tianjin, China.

doi:10.56397/SLJ.2025.02.08

**Abstract**

The widespread popularity of smart wearable devices has brought convenience to personal health management, but it has also raised challenges in the protection of personal health information security. This paper conducts research by comprehensively applying methods such as literature collection, empirical analysis, and comparative law research. Through a questionnaire survey, it is found that different groups have different understandings of personal information protection under smart wearable technology, and there are many problems in aspects such as information collection consent and anonymization processing. Meanwhile, the research points out that personal health information under smart wearable technology faces risks such as unnoticed information leakage risks, difficulties in controlling information uses that lead to rights and interest's crises, and doubts about the effectiveness of anonymization processing. There are also dilemmas in legal definition, legislation, supervision, and judicial practice. Therefore, it is recommended to incorporate smart wearable devices into medical device supervision and establish a certification mechanism, implement the dynamic consent rule based on the purpose of information processing, promote algorithm transparency, and improve the tort liability system, so as to build a protection system for personal health information and achieve a win-win situation between the development of smart wearable technology and the protection of personal rights and interests.

**Keywords:** smart wearable devices, personal health information, information security risks, dilemmas in legal protection, dynamic consent rule, construction of protection system

## 1. Introduction

### *1.1 The Increasing Popularity of Smart Wearable Devices*

Smart wearable devices, a type of miniature electronic devices that can be worn on the human body and are convenient for use during outdoor activities, usually consist of components such as sensors, display screens, and algorithms for data processing. Through the coordinated operation of these components, smart wearable devices can accurately measure various vital signs, covering key health indicators such as body temperature, heart rate, blood pressure, and blood oxygen saturation.

At present, the popularity of smart wearable

devices is growing day by day, and a considerable number of people use such devices daily. Well-known manufacturers represented by Apple and Xiaomi are continuously increasing their market share in the smart wearable device market. However, with the rapid development of this industry, a series of problems have gradually emerged.

*1.2 Smart Wearable Devices Pose Challenges to the Protection of Personal Health Information Security*

In the field of personal health management, smart wearable technology is being applied more and more widely. With its remarkable advantages of portability and real-time performance, it provides users with a more convenient health monitoring experience. However, along with it, the security risks of personal health information are gradually emerging, making the management and protection of personal health information under smart wearable technology an important topic that urgently needs in-depth research at present.

The data collected by smart wearable devices directly reflects the health status of users and should be classified into the category of personal health information and be strictly protected by law. At present, it is not easy to strike a balance between promoting the development of related industries and protecting user privacy, and many legal issues need to be resolved urgently. Against this background, how to give full play to the advantages of smart wearable technology in health management on the basis of ensuring user privacy has become a major challenge in this field.

*1.3 Research Significance*

In-depth research on personal health information under smart wearable technology is of great significance. It can not only promote the continuous optimization of the functions and performance of smart wearable devices and provide support for technological progress but also provide theoretical support and practical guidance for the innovative development of health management, helping to build a more complete, efficient, and secure health management system.

1.3.1 The Dynamic Consent Rule Provides a New Theoretical Perspective for the Protection of Personal Health Information

Currently, the protection of personal health information faces many problems. One of them is that the definition of personal health information is not clear, which makes it difficult to effectively implement the separate consent rule and the full-necessity rule stipulated in the Personal Information Protection Law in practice. Therefore, applying the dynamic consent rule based on the purpose of information processing provides an important way to solve this problem. This paper puts forward new understandings and solutions to issues related to the "separate consent rule" and the premise of "full-necessity". In particular, the introduction of the concept of the "dynamic consent rule" makes up for the deficiencies of traditional "static" methods and provides new theoretical support and methodology for more comprehensive and perfect protection of personal health information.

1.3.2 Exploring the Legal Protection Mechanism for Personal Health Information Contributes to the Construction of a Healthy China

The rapid development of smart wearable technology has had a significant impact on the security of citizens' personal information and the national public health system. Although the Civil Code of China and the Personal Information Protection Law of China have stipulated the protection of personal health information, there are still some deficiencies in practice.

Therefore, it is urgent to explore a legal protection mechanism for personal health information that conforms to the characteristics of the new era. This can not only standardize the circulation of personal health data to ensure legal and orderly transfer, but also tap its potential value for benign utilization, providing legal guarantee for the construction of a "Healthy China".

*1.4 Review of Foreign Research Status*

Professor Fred Cate from Indiana University in the United States pointed out that consent notices for current smart wearable devices have significant flaws. These notices are either too general or overly detailed and complex. This undermines users' ability to make "conscious choices". In other words, users can't make decisions according to their will because they lack a full understanding. Additionally, such notices often mislead users into believing their privacy is well-protected, when in fact, their personal information may be at risk unbeknownst to them.

Surveys funded by the National Research Foundation of South Africa show that two-thirds of wearable device users do not understand the health information stored or transmitted by the devices. 43.40% of users are unclear about the data transmission encryption methods, and over half of the respondents do not know who to contact in case of information security issues. This indicates that users have a low level of privacy awareness and blindly trust that their data is protected, which may lead to confusion over liability in case of data breaches. This current situation not only poses a potential threat to users' personal information security but also plants hidden dangers for the healthy development of the entire wearable device industry.

The Pew Research Center pointed out in its research report focusing on privacy and information sharing that the majority of American adults believe that wearable devices damage consumers' privacy. Respondents generally feel that they are being monitored, and few people think they have much decision-making power over the personal health information collected by smart wearable devices and how this information is used. This shows that people are worried and distrustful about the current state of protection of personal health information in smart wearable devices.

## 2. Methods

### *2.1 Analytical Research Methods and Search Strategies*

This research comprehensively applies various methods such as literature collection, empirical analysis, and comparative research to comprehensively analyze the current situation and problems of personal health information protection in smart wearable devices and explore feasible protection paths. To obtain rich and in- depth research materials, team members conducted extensive searches in professional databases such as HeinOnline, JSTOR, Springer, and CNKI, as well as in the Google Scholar search engine, using keywords closely related to the article's theme.

### *2.2 Data Collection Methods and Situations*

In order to initially understand the awareness of different groups regarding personal information protection under smart wearable technology, the relevant personnel of this project carried out a survey in the form of a questionnaire on this issue. Through preliminary research, a total of 320 questionnaires were collected, among which 320 were valid samples.

## 3. Results

### *3.1 Data Collection Situations*

This research conducted data collection and analysis on the use of smart wearable devices and related situations of personal health information. The specific results are as follows:

#### 3.1.1 Distribution of Respondents by Gender and Age

Among the respondents participating in the survey, the gender ratio is 67.81% for females and 32.19% for males. In terms of age distribution, respondents under 18 years old account for the largest proportion, reaching 67.19%; those aged 18 – 24 account for 25.94%; those aged 25 – 45 account for 3.75%; and those over 45 years old account for 3.13%.

#### 3.1.2 Current Situation and Usage of Smart Wearable Devices

The survey shows that 62.81% of the respondents are using smart wearable devices. In terms of usage, checking the time, monitoring exercise steps, and receiving message reminders are the most important functions, and the usage rates of these three functions all exceed 50%.

#### 3.1.3 Respondents' Cognition of Personal Health Information

Respondents had different opinions on which data were considered personal health information. More than 80% of the respondents believed that blood pressure and heart rate were personal health information. The recognition rates for sleep time and eating habits were 72.96% and 67.47% respectively. For other data, less than 60% of the respondents recognized them as personal health information. In addition, regarding the connection between the information collected by smart wearable devices and personal health conditions, 57.88% of the respondents thought they were closely related, 31.51% of the respondents said they didn't know much about it, and 10.62% of the respondents thought there was no connection.

#### 3.1.4 User Consent Regarding Information Collection by Operators

Regarding whether operators obtain explicit consent from users when collecting information, 25.34% of the respondents pointed out that they did not give consent. 50% of the respondents said that operators provided standard contract

terms, but they themselves did not read them carefully. Only 24.66% of the respondents claimed to have carefully read the standard contract terms.

3.1.5 Respondents' Understanding and Acceptance of Information Anonymization

In terms of information anonymization, 43.15% of the respondents were not clear about its specific procedures. 28.08% of the respondents said they had sufficient understanding, and 28.77% of the respondents had only heard of "anonymization" but did not know much about it. Regarding the use of anonymized information by enterprises, 55.82% of the respondents said they could accept it, 21.23% of the respondents clearly stated that they could not accept it, and 22.95% of the respondents had an open-minded attitude.

*3.2 Overseas Legislative Situations*

3.2.1 The United States

The "Consumer Privacy Protection Act of 2015" issued by the United States clearly defined the scope of "sensitive personal identifying information" in Section 3. It includes "unique biometric data, such as faceprint, fingerprint, voice print, a retina or iris image", as well as "any information that relates to the individual's past, present, or future physical or mental health or condition".

3.2.2 The European Union

In 2016, the General Data Protection Regulation (GDPR) promulgated by the European Union clearly defined the scope of health-related personal data. The regulation stipulates that all data related to the health status of the data subject fall within the scope of protection. Specifically, if these data can reflect the physiological or biomedical state information of the data subject, regardless of their source (even if they come from medical devices or in - vitro diagnostic tests, etc.), they should be given corresponding protection.

3.2.3 Japan and Taiwan, China

Japan's "Act on the Protection of Personal Information" classifies medical information as a category of personal information that requires special consideration. It includes medical history, physical examination results, medical advice, etc. The "Personal Data Protection Act" in Taiwan region of China clearly prohibits the collection, processing, and utilization of personal information closely related to personal health conditions, such as medical records, medical information, and health check-ups.

**4. Discussion**

*4.1 Risks Faced by Personal Health Information Under Smart Wearable Technology*

4.1.1 The Overlooked Risk of Information Leakage

Both smart wearable devices and smartphones have the functions of recording personal activity trajectories and collecting health information, but there are significant differences between them in terms of information leakage risks. Devices such as smartphones require users to actively operate them. Users can more intuitively perceive the potential risks during the operation process and thus take corresponding preventive measures.

In sharp contrast, smart wearable devices, often relying on their convenience and the feature of being worn close to the body, continuously collect various types of information without the user's awareness. Due to their daily and concealed use, users often overlook their data collection behavior during the wearing process. Unconsciously, users change from active controllers of information to passive producers of information, making it difficult to effectively supervise the flow and use of information. As a result, personal health information faces a greater risk of leakage.

4.1.2 Crisis of Rights and Interests Caused by Difficulty in Controlling Information Use

There is a problem of difficulty in controlling the use of personal health information collected by smart wearable devices. The insurance industry is a typical example. Insurance companies may obtain health data from smart wearable devices in order to more accurately assess the risks of policyholders. On the surface, by using these data, insurance companies can set premium prices that better match the actual risk status of policyholders, achieving an accurate match between risk and premium.

However, upon in-depth analysis, it can be found that this way of using data may bring a series of negative impacts. For people with poor health, the data collected by smart wearable devices may put them under greater pressure in terms of insurance premiums. This differential treatment based on health information is essentially a discriminatory practice, which goes against the original intention of data collection.

It turns the data from a tool for safeguarding users' rights and interests into a source of damage to the rights and interests of some users.

4.1.3 Doubts About the Effectiveness of Anonymization

China's "Personal Information Protection Law" stipulates that information processed through anonymization no longer belongs to the category of personal information. Anonymization refers to the processing of personal information through technical means so that it cannot identify a specific natural person, and the original identity cannot be restored. However, in practical applications, anonymization technology is not foolproof. Research by the University of Texas in the United States shows that if an attacker has a certain understanding of the user, it is relatively easy to identify the user's anonymized data records, at least a small part of the data. Thus, relying solely on anonymizing the information collected by smart wearable devices cannot build a reliable defense line against risks for personal health information.

*4.2 The Definition and Development of Personal Health Information Under Smart Wearable Technology*

4.2.1 The Current Status of the Definition of Personal Health Information

4.2.1.1 Analysis of the Current Status of the Definition of Personal Health Information

In China's current legal system, there are many provisions involving the protection of medical and health information. For example, the "Law on the Prevention and Treatment of Infectious Diseases" revised in 2013 gives specific institutions the power to collect information related to infectious diseases and requires the protection of personal privacy information therein. The "Mental Health Law" revised in 2018 also clearly stipulates the obligation to keep confidential the personal information of patients with mental disorders.

However, these laws have obvious ambiguity in the specific definition of medical and health information. In 2020, the Civil Code classified "health information" into the category of "personal information" for protection, but its connotation was not clearly defined. Although the "Personal Information Protection Law" in 2021 strengthened the protection of "personal health information", it still did not solve the problems of unclear definition and ambiguous standards, which has brought difficulties to the specific implementation of the law and the accurate protection of personal health information.

4.2.1.2 Insight into Overseas Legislative Trends

Countries and regions are increasingly refining the definition of personal health information. It is no longer limited to traditional medical data. For example, the United States includes unique biometric data in the scope of protection. The European Union covers all information that can reflect physiological or biomedical states. Japan focuses on various specific information under the category of medical information. In Taiwan region of China, case records, health examination and other information are clearly enumerated. This comprehensive and detailed definition clarifies the protected objects, reduces ambiguous areas, and better safeguards personal rights and interests.

The protection intensity is also continuously enhanced. In the United States, relevant information is classified as "sensitive personally identifiable information." The European Union stipulates that data related to health conditions are all protected. Japan gives special consideration to medical information. In Taiwan region of China, improper utilization behaviors such as collection are directly prohibited. From different angles, the protection standards are raised, the constraints on infringement acts are increased, and the security of personal health information is guaranteed.

Although legislative models vary from place to place, they all adhere to the core concept of protecting privacy and standardizing data processing. While safeguarding personal rights and interests, they also consider the rational use of data and the development of related industries.

4.2.2 The Dynamic Development Trend of the Definition of Personal Health Information

4.2.2.1 The Definition Change Triggered by Smart Wearable Technology

Smart wearable technology can create personalized data archives and continuously record users' activity information through sensors and internet feedback. Affected by smart wearable technology, the concept of personal health information has undergone significant changes and no longer has a clearly defined and

stable boundary in the traditional sense. Some originally ordinary personal information may be transformed into personal health information after processing.

For example, information such as daily step count, standing duration, and social media usage collected by smart wearable devices may seem to have no direct connection with health, but in fact, there is an indirect association. Through statistical analysis, this information can reveal potential relationships with health and provide support for health trend prediction. A low daily step count may mean insufficient exercise, increasing the risk of chronic diseases; a too short standing duration reflects poor physical endurance and muscle strength; a low communication frequency may imply psychological loneliness and affect mental health.

4.2.2.2 Exploration of Legal Paths Based on Comparative Law

Drawing on the legislative ideas of the United States and the European Union, the key to determining whether personal data belongs to personal health status information lies in its intended use. Even data that appears to be unrelated to health on the surface should be subject to corresponding restrictions and protection if it is used to infer an individual's health condition.

This shows that the definition of personal health information is dynamically changing. To determine whether an item of information belongs to personal health information, one cannot rely solely on the characteristics of the information itself. The purpose for which the information is used also needs to be considered. Some information that cannot directly reflect health content should be regarded as personal health information if it can be used to reasonably infer an individual's health status. This "dynamic" definition method makes up for the deficiency of "static" definition and can protect personal health information more comprehensively.

*4.3 The Legal Dilemmas of Personal Health Information Protection Under Smart Wearable Technology*

4.3.1 Difficulties in Legislation

4.3.1.1 The Ambiguous Definition of Personal Health Information Makes Effective Protection Difficult

In China's current legal system, the concept and scope of "personal health information" and its protection boundaries have not been clearly and accurately defined. This legislative ambiguity makes it difficult for relevant laws to effectively play their regulatory and guarantee roles in specific judicial practices and rights protection processes.

With the rapid development of smart wearable technology, diversified devices such as smart bracelets and smart watches are widely popularized, and the types of information they collect and generate are complex and diverse. However, there is great controversy in both academic and practical fields as to whether the information collected and generated by these devices should be included in the legal category of personal health information. Taking the sleep duration and heart rate fluctuation data recorded by smart wearable devices as an example, from a medical professional perspective, such data can reflect an individual's health status to a certain extent. However, since the collectors are not traditional medical institutions with professional qualifications, under the current legal framework, there are many obstacles in determining these pieces of information as sensitive information, and it is difficult for them to receive adequate legal protection.

4.3.1.2 Obstruction in the Actual Implementation of Separate Consent and Sufficiency-Necessity Rules

According to the provisions of the "Personal Information Protection Law", processing sensitive personal information requires obtaining the individual's separate consent and meeting the precondition of "sufficiency and necessity". Among them, the separate consent rules require the information processor to provide separate and clear notification to the information subject on key elements such as processing purpose, method, scope, and obtain their explicit consent expression, to fully guarantee the information subject's right to know and decision-making power regarding the processing of their own information. The "sufficiency and necessity" condition emphasizes that processing sensitive personal information must be an indispensable measure for achieving a specific purpose. Compared with the "direct relevance" required for ordinary information processing, its standard is stricter.

However, in the actual application scenarios of smart wearable devices, due to their daily use and convenience, many devices obtain user authorization through long and complex terms and conditions in the form of blanket consent when they are first activated. This consent notice is often written too broadly or in too much detail, making it difficult for users to understand and not actually a conscious choice. Enterprises thus achieve the purpose of circumventing the application of the separate consent rules. At the same time, some enterprises apply the massive amount of personal information collected by smart wearable devices to fields such as health analysis and even commercial marketing without distinction and recklessly. This clearly goes far beyond the reasonable boundary of "sufficiency and necessity" and seriously violates the relevant legal provisions on the protection of personal sensitive information, making these two crucial legal rules difficult to be effectively implemented in practice.

4.3.2 The Dilemmas of the Subjects and Responsibilities in Administrative Supervision

4.3.2.1 The Confusion of Regulatory Subjects Leads to the Dilemma of Individual Rights Protection

According to Article 60 of the "Personal Information Protection Law", the national cyberspace administration undertakes the responsibility of overall coordination in personal information protection work. Other relevant functional departments, such as the Ministry of Industry and Information Technology and the health department, implement specific supervision over personal information protection work within their respective legal responsibilities. As an emerging information collection terminal, smart wearable devices generate and collect information that widely involves multiple fields such as network information security, health, and insurance. However, at present, the boundaries of regulatory responsibilities among various departments lack clear and detailed divisions, and there are many ambiguous areas and overlapping regions.

When personal health information collected by smart wearable devices is leaked, the information subject often finds it difficult to determine which specific department to complain to and defend their rights. Reporting the situation to the network supervision department may result in being told that this matter involves health data and should seek a solution from the health department. However, the health department may think that this problem involves the network transmission link and is not within its scope of responsibilities. This chaotic situation of regulatory subjects, coupled with the ambiguity in the legal definition of personal health information itself, makes it difficult to effectively carry out supervision and protection work. When the legitimate rights and interests of information subjects are violated, it is difficult for them to obtain timely and effective remedies through normal administrative channels.

4.3.2.2 Unclear Regulatory Responsibilities Hinder the Implementation of Regulatory Work

The "State Measures for the Management of the Standard, Security and Services of Medical and Health-related Big Data (Trial)" clearly stipulates that the National Health Commission is responsible for the supervision and management of health and medical big data, including responsibilities such as regularly conducting relevant inspections, implementing risk assessments, and imposing penalties on violations. However, this measure has obvious defects at the practical implementation level. For the specific content of inspections, the detailed standards for risk assessment, and the accurate scope of regulatory objects, no clear and specific regulations have been made.

With the continuous iterative upgrade of smart wearable technology, new device functions and data collection methods continue to emerge. If the responsibilities of the regulatory subject are still in an ambiguous state, then when facing massive amounts of smart wearable devices and the personal health information they generate, regulatory departments will find it difficult to formulate scientific and effective regulatory strategies and implementation plans. Regulatory work is extremely likely to become a mere formality and cannot effectively achieve the goal of protection of personal health information.

4.3.3 Challenges Faced by Judicial Practice

4.3.3.1 Unclear Legal Basis Leading to Discrepancies in Judicial Decisions

Due to the lack of clear legal definitions and specific criteria or applicable rules regarding personal health information, judges, when handling related cases, are often forced to exercise discretion based on their own

professional knowledge and judicial experience. As a result, when faced with factually similar cases, different judges may reach drastically different verdicts based on varying interpretations and assessments of the law.

Although the number of judicial rulings involving personal health information under wearable technology is still relatively limited, similar cases of significant differences in verdicts due to unclear legal standards are already common in other sensitive information domains. For instance, in cases involving "location tracking" information infringement, some courts believe that any information that can roughly identify an individual's location should be classified as sensitive, with the infringer facing stricter legal responsibility. However, other courts argue that a more comprehensive assessment is necessary, considering factors such as the specific context of use and the precision of the information, before making an accurate judgment. This leads to significant discrepancies in judicial outcomes. In the fast-evolving era of wearable technology, this lack of clear legal definition will undoubtedly expand the discretion available to judges, making it difficult for information subjects to obtain stable and consistent judicial remedies for their legitimate rights.

4.3.3.2 Difficulty in Determining Tort Liability Due to Complex Causal Relationships

In personal information infringement cases, particularly those involving smart wearable devices, the issue is often closely linked to the dissemination and application of big data, which makes the causal relationship between the infringing act and the resulting harm highly complex. In the process of collecting and generating personal health information, smart wearable devices typically go through multiple stages, such as data collection, transmission, storage, and analysis, with each stage potentially involving security risks and vulnerabilities.

For example, a user's health data may be illegally accessed on the device end, intercepted by hackers during transmission, or leaked due to poor management by the storage provider. At the same time, in recent years, the risks to personal privacy have been escalating, with the leakage of personal health information potentially resulting from a combination of factors, such as security flaws in the wearable device itself, unauthorized access by third-party applications, or even improper user actions in insecure network environments. When the data subject faces an infringement risk, accurately identifying the exact party responsible for the violation among numerous potential harmful factors is a significant challenge. This undoubtedly presents a severe challenge for determining tort liability in judicial practice.

## 5. Recommendations for Building a Personal Health Information Protection System

Building a comprehensive and effective protection system is not only a strong safeguard for users' rights but also a key factor in ensuring the healthy and sustainable development of the smart wearable industry. To this end, we can collaborate across three critical levels — national, industry, and consumer rights — to create an all-encompassing protection system.

### *5.1 Incorporating Smart Wearable Devices into Medical Device Regulation and Establishing a Certification Mechanism*

Smart wearable devices, with their powerful functions, have become valuable tools for personal health management. However, the vast amounts of personal health information they collect also pose significant security risks. From an international development perspective, the United States has proactively included smart wearable devices under the definition of medical devices in its relevant legislation. This move provides a strong legal basis for strict regulation of smart wearables, ensuring the protection of citizens' health information security. China can also follow this trend and precisely incorporate smart wearable devices into the medical device regulatory framework.

At the same time, the European Union's well-established certification system provides valuable lessons for us. We can draw from the EU model to establish a professional and authoritative data protection certification body. The responsibilities of this body would cover several key aspects. On one hand, it should conduct rigorous compliance checks on device manufacturers, ensuring that device quality and information security standards are controlled from the production source. On the other hand, it should carefully evaluate the intended use of the devices to prevent misuse. Additionally, the body should conduct comprehensive and in-depth assessments of the potential risks to information security and privacy protection posed by the devices. Through these measures,

we can establish a certification mechanism suitable for China, thereby comprehensively safeguarding the security of personal health information.

*5.2 Implementing Dynamic Consent Rules Based on Information Processing Purposes*

Under the constraints of the Personal Information Protection Law, information processors must strictly implement dynamic consent rules based on the different purposes of information processing. Due to algorithmic technologies blurring the boundaries between different types of information, ordinary life data can easily be transformed into sensitive personal health information after algorithmic analysis in today's technological environment. For example, seemingly ordinary life data such as daily step counts and sleep duration, once subjected to deep analysis by advanced algorithms, may accurately reflect an individual's physical condition, thereby becoming health information.

When the information processor is handling only personal lifestyle information, obtaining general consent from the user is sufficient. However, once the processing involves highly sensitive areas such as personal health assessments or disease risk predictions, the information processor is responsible for providing clear and explicit notifications to the user. This includes informing the user of the purpose, methods, and potential risks of information processing, and obtaining separate consent from the user. Through this differentiated dynamic consent rule, users' right to be informed about the processing of their personal information is fully protected, ensuring that users remain in an active and controllable position throughout the information processing process.

*5.3 Promoting Algorithm Transparency and Improving Tort Liability System*

In the complex process of information processing by smart wearable devices, algorithms undoubtedly play a central and crucial role. They act as the "behind-the-scenes operator," determining the direction and outcome of information processing. Promoting algorithm transparency is essential for ensuring that consumers can effectively exercise their right to informed consent. If consumers are unaware that their information is being collected or how it is being used, they are unable to make choices that are in their best interest. Only when consumers have a clear understanding of the algorithm's operational logic, data processing methods, and potential impacts can they make decisions that truly reflect their own preferences.

However, with the widespread use of algorithms in the processing of personal health information, issues of infringement are becoming increasingly prominent. To effectively address this challenge, improving the tort liability system is imperative. We should clarify the principle of strict liability, considering that personal information infringements often have characteristics such as being collective and covert. Adopting a strict liability principle will more effectively protect individuals' information rights. Even if no actual harm has occurred, as long as there is illegal collection, improper use, or disclosure of personal health information, the infringing party should bear corresponding legal responsibility. Through such a clear liability framework, we can deter potential infringers to the greatest extent and foster a healthy and secure information processing environment.

**6. Conclusion**

The rise of smart wearable technology has brought about both transformative opportunities and challenges in the protection of personal health information, from concept to practice. While the widespread use of device-collected data has facilitated personal health management, it has also raised significant privacy and security concerns. Currently, there are urgent issues in the legal framework concerning the definition of personal health information, processing rules, and regulatory enforcement, which directly affect both the protection of individual rights and the healthy development of the industry.

The protection of personal health information is a complex, systemic endeavor that requires the collective efforts of the government, industry, businesses, and consumers. In the future, as technology continues to evolve, it is essential to remain attentive to emerging issues and continuously improve relevant laws, regulations, and regulatory mechanisms. This will ensure the security of personal health information while promoting the healthy development of smart wearable technology in the field of health management, ultimately achieving a win-win situation for technological

progress and the protection of individual rights.

**References**


Arnow, G. (2016). Apple Watch-ing You: Why Wearable Technology Should be Federally Regulated. *Loyola of Los Angeles Law Review*, *49*(3), 607-634. https://digitalcommons.lmu.edu/llr/vol49/iss3/2.

Banerjee, S. (Sy), Hemphill, T. and Longstreet, P. (2017). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 1-9. https://doi.org/10.1080/01972243.2017.1391912.

Banerjee, S. (Sy), Hemphill, T. A. and Longstreet, P. (2021). Is IoT a threat to consumer consent? The perils of wearable devices' health data exposure. *Journal of Cybersecurity and Privacy*, *15*(3), 45-67. http://dx.doi.org/10.1080/15564365.2021.978000.

Beranek Lafky, D., Horan, T. A. (2011). Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health Informatics Journal*, *17*(I), 63-71. https://doi.org/10.1177/1460458211399403.

Bouderhem, R. (2023). Privacy and Regulatory Issues in Wearable Health Technology. *Eng. Proc*, *58*, 87. https://doi.org/10.3390/ecsa-10-16206.

Cate, F. H. (2010). Protecting Privacy in Health Research: The Limits of Individual Choice. *California Law Review*, *98*, 1765-1804. https://www.repository.law.indiana.edu/facpub/235.

Chan, M., Estève, D., Fourniols, J.-Y., Escriba, C. and Campo, E. (2012). Smart wearable systems: Current status and future challenges. *Artificial Intelligence in Medicine*, *56*(3), 137-156. https://doi.org/10.1016/j.artmed.2012.09.003.

Cilliers, L. (2019). Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal*, 1-7. https://doi.org/10.1177/1833358319851684.

Consumer Privacy Protection Act of 2015. (2015). 114th Congress, Senate Bill 1158. https://www.congress.gov/bill/114th-congress/senate-bill/1158/text.

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *Journal of Law, Medicine & Ethics*, *46*(4), 1013-1030. https://doi.org/10.1177/1073110518822003.

Feng, Y., Agosto, D. E. (2019). From health to performance: Amateur runners' personal health information management with activity tracking technology. *Personal Health Information Management*, *71*(2), 217-240. https://doi.org/10.1108/AJIM-07-2018-0170.

Hiller, J., McMullen, M. S., Chumney, W. M. and Baumer, D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): U.S. and EU compared. *Boston University Journal of Science & Technology Law*, *17*(1), 1-39. https://vtechworks.lib.vt.edu/server/api/core/bitstreams/637d5744-72d4-4cd2-83a8-10d034e14b87/content.

Ioannidou, I., Sklavos, N. (2021). On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography*, *5*(4), 29. https://doi.org/10.3390/cryptography5040029.

Japan. (2003). Act on the Protection of Personal Information (Partly unenforced). (2003). Act No. 57 of May 30, 2003. https://www.japaneselawtranslation.go.jp/en/laws/view/424/en.

Klimoski, R., Palmer, S. (1993). ADA and the hiring process in organizations. *Consulting Psychology Journal: Practice and Research*, *45*(2), 10-36. https://www.jmir.org/2023/1/e41635.

Mason Marks. (2021). Emergent Medical Data: Health Information Inferred by Artificial Intelligence. *UC Irvine Law Review*, *11*(4), 995. https://scholarship.law.uci.edu/ucilr/vol11/iss4/7.

Ohm, P. (2009-2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, *57*, 1701. https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclalr57&div=48&id=&page=.

Pasquale, F. (2014). Redescribing Health Privacy:

The Importance of Information Policy. *Houston Journal of Health Law & Policy*, *14*, 1-28. https://scholarship.law.uci.edu/ucilr/vol11/iss4/7.

Pasquale, F. (2023). Health Data on the Go: Navigating Privacy Concerns with Wearable Technologies. *Legal Information Management*, *23*, 179-188. https://doi.org/10.1017/S1472669623000427.

Rainie, L., Duggan, M. (2016, January 14). Privacy and Information Sharing. Pew Research Center. https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/.

Regulation (EU) 2016/679. (2016). On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, *L*, *119*, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Spila, T., Kleinb, R. (2015). The personal health future. *Health Policy and Technology*, *4*(2), 131-136. https://doi.org/10.1016/j.hlpt.2015.02.004.

Terry, N. P., Wiley, L. F. (2016). Liability for mobile health and wearable technologies. *Annals of Health Law*, *25*(2), 62-97. https://digitalcommons.wcl.american.edu/facsch_lawrev/1170/.

Vezyridis, P., Timmons, S. (2015). On the adoption of personal health records: some problematic issues for patient empowerment. *Ethics in Technology*, *17*, 113-124. https://doi.org/10.1007/s10676-015-9365-x.

Ziccardi, G. (2012). Wearable Technologies and Smart Clothing in the Fashion Business: Cybersecurity and Data Protection Issues. *Laws*, *9*(2), 12. https://doi.org/10.3390/laws9020012.