International Journal of Humanities Social Sciences and Education (IJHSSE)
Volume 11, Issue 4, April 2024, PP 47-60
ISSN 2349-0373 (Print) & ISSN 2349-0381 (Online)
https://doi.org/10.20431/2349-0381.1104004
www.arcjournals.org

A Preliminary Study on the Accountabilities and Risks of Wise Information Technology of Medicine in Taiwan

Wen-Chuan Ke

PhD Researcher Fellow, Department of Industrial Education, National Taiwan Normal University; Adjunct Associate Professor, Department of Industrial Engineering and Management, National Taipei University of Technology; Adjunct Associate Professor, Department of Public Administration, National Open University.

Corresponding Author:** ***Wen-Chuan Ke, *PhD Researcher Fellow, Department of Industrial Education, National Taiwan Normal University; Adjunct Associate Professor, Department of Industrial Engineering and Management, National Taipei University of Technology; Adjunct Associate Professor, Department of Public Administration, National Open University.*

Abstract: *When AI becomes an accelerator under the wave of big data, comprehensive countermeasures should establish separate regulations for the use of data in the AI era, such as the General Data Protection Regulation (GDPR) implemented by the European Union in 2018, which is an important indicator of personal data protection in the AI era. If there is a problem of discrimination in the relevant AI application field, it is necessary to further implement the accountability of AI, and at the same time prevent the social risks caused by the abuse of artificial intelligence technology.*

In the medical field, AI technology is currently playing an auxiliary role to assist medical staff, so that medical information and solutions can be further integrated through AI medical technology. Through the discussion on the accountability of Wise Information Technology of Medicine, further thinking about the implementation of the accountability is the most important task. As far as the accountability of Wise Information Technology of Medicine is concerned, it seems that several situations can be used to discuss the clinical problems and accountability. First, the product liability issue, the solution is the discussion of legal protection and regulatory concurrence; Second, the patient safety issue, the solution is the establishment of a regulatory sandbox system; Third, the black box problem caused by the algorithm, the solution for the establishment of norms; Fourth, the privacy and differential treatment caused by biological information, the solution is the specific implementation of personal data protection; Fifth, the problem of genetic information being exposed in large quantities, the solution is the establishment of an information security system.

In order to prevent the risks caused by the abuse of artificial intelligence technology, through the discussion of related risk issues in Wise Information Technology of Medicine, starting from the safety of different risk levels, the software design and development life cycle are developed, and the experience of the European Union and the United States can be used to evaluate Possible risks and directions for response. Furthermore, due to the promotion of Wise Information Technology of Medicine, the storage and use of a large amount of data will inevitably be required. How to balance personal data protection and full use of data is also an important topic of discussion. This part seems to be able to learn from the experience of other countries, such as EHDS, GDPR, etc.

Keywords: *Wise Information Technology of Medicine, informed consent, privacy, genetic information, accountability, risk assessment.*

1. PREFACE

The algorithm breakthrough brought about by artificial intelligence in deep learning not only promotes the continuous development of integrated circuits, but also promotes the development of Wise Information Technology of Medicine. In addition to being based on medical data, Wise Information Technology of Medicine is also the key to algorithmic decision-making. However, the AI medical system developed by machine learning algorithms inevitably has a black box problem, making it impossible for users of AI medical applications to know the calculation process and influencing factors of medical judgments and decision results, and it may even be because the AI system involves business secrets The refusal of the product manufacturer to disclose the details of the algorithm may also cause the doctor to use the AI system to be unable to inform the patient of the basis for judging the condition, and thus unable to fulfill the obligation of informing and consenting.

The medical and health data used by AI medical care specifically includes medical records such as medical records, medical records, surgery, and hospital care in medical institutions, as well as biological data such as specimens and genes, as well as labor health examination records and national health insurance records. Declaration documents, and wearable devices and medical mobile applications that record personal physiological status. The particularity of these data is that it is easy to reveal personal psychological or physical private information. For example, in the treatment reports on psychological medicine or sexually transmitted diseases, personal friendships may be disclosed; or medical images of health examinations may reveal general personal information. The most private parts of the body and diseases; for example, the health information disclosed by genetic information may affect personal employment, schooling, insurance, etc., resulting in privacy and differential treatment issues.

In addition, genetic information can be used to identify personal characteristics and be used for disease analysis, treatment, prescribing, or as the basis for fertility counseling, and it is also considered to have great potential benefits in business. With the advancement of biomedical technology, even the genetic map of the entire family can be known from individual tiny genes. Coupled with the advancement of AI technology, the personal information that can be revealed by relying on AI calculations is beyond the imagination of ordinary people. So far, the privacy risks caused by AI medical care are not limited to individuals, but can also extend from personal data privacy risks to social impacts such as ethnic groups and races.

Based on the discussion of the responsibilities and related risk issues of risk-based smart medical care, this article further considers the implementation of responsibilities and evaluates the possible consequences and response directions.

2. The accountability of Wise Information Technology of Medicine

In the medical field, AI technology is currently playing an auxiliary role to assist medical staff, so that medical information and solutions can be further integrated through AI medical technology. For example, the AI medical diagnosis system can classify and stratify medical and health information such as patient life medical information and medical records, provide data-oriented diagnosis and prediction, suggest relevant treatment plans or propose treatment procedures, and assist in the procedures to be followed during the operation The procedure evaluates the risks during surgery and the chances of survival.

Accountability means that members of an organization must accept rewards or punishments for decisions or actions, and each level has the obligation to be supervised. It is an external judgment standard, which is, external calculation or obedience. Class accountability management is oriented by the results of the organization, and attaches great importance to the degree of making good use of limited resources in the process, and finally emphasizes the implementation of their own decision-making accountabilities. However, there are still a few points to note:

First, Transparency: The business content and achievements should be clearly listed so that the accountability of the course is based on the basis.

Second, Personal aspect: accountability must ultimately be implemented on the individual, not the highest level of the organization.

Third, Retrospective: Through the feedback of performance information, public managers can really take accountability for the results of their actions.

Far as the accountabilities of Wise Information Technology of Medicine are concerned , it seems possible to proceed from the following situations to discuss the problems and accountabilities faced by clinical practice.

3. Discussion on Product Liability

3.1. Product Liability

Although AI medical care does not have a certain physical form and cannot be classified as a product, it can still be classified as a service and is subject to the application of consumer protection laws. According to Article 7 of the Consumer Protection Act: Business operators engaged in the provision

of services shall ensure that the services comply with the safety that can be reasonably expected at the current technological or professional level when providing services. If the business operator violates the regulations and causes damage to consumers or third parties, he shall be liable for joint and several damages. It can be seen that "no-fault liability" is adopted for business operators.

In addition, the Pharmaceutical Affairs Act has separated the management of medical devices from the Pharmaceutical Affairs Law. Article 3 of Enforcement Rules of Medical Devices Act stipulates: Medical devices refer to medical devices that are used to diagnose, treat, mitigate, directly prevent human diseases, regulate fertility, or affect human body structure and functions, and do not act on the human body through pharmacological, immune or metabolic methods. , Instruments, devices, utensils, substances, software, in vitro reagents and related items to achieve their main functions. AI medical treatment meets the software requirements of Article 3 of the Pharmaceutical Affairs Act and should be a medical device. Article 8 and Article 82 of the Pharmaceutical Affairs Act stipulate that the liability of medical device manufacturers and importers is based on presumed negligence. According to Article 8 of Enforcement Rules of Medical Devices Act, bad medical devices refer to medical devices that have been inspected or inspected to cause errors in diagnosis, or contain poisonous or harmful substances that endanger human health; If the equipment is defective, the patient may claim compensation for damages from the manufacturer or importer of the medical equipment.

Furthermore, according to Article 191-1 of the Civil Code, the manufacturer of a product is liable for damages caused by the normal use or consumption of the product to others. However, unless there is no defect in the production, manufacture, processing, or design of the product, or the damage is not caused by such defect, or if considerable care has been taken in the occurrence of the damage, the "presumptive negligence liability" shall be adopted.

3.2. Solution: Legal Protection and Regulatory Concurrence

3.2.1. Competition and Cooperation between Consumer Protection Law, Civil Law and Pharmaceutical Affairs Act

The law has the principle that special law is superior to common law. According to Article 16 of the Central Regulations and Standards Act: Regulations that have special provisions for the same matters stipulated in other regulations shall take precedence. Therefore, since the Pharmaceutical Affairs Act has special provisions for medical devices, it should be applied first.

3.2.2. Competition and Cooperation between Civil Law and Consumer Protection Law

If Wise Information Technology of Medicine is applicable to Article 7 of the Consumer Protection Law and Article 191-1 of the Civil Code, and there is a conflict of application, there are three theories, as follows:

The Theory of Competition and Cooperation of Laws and Regulations

The consumer protection law is regarded as a special law of civil law, and the principle of applying special law takes precedence over common law. Therefore, when the facts of the case meet the requirements of both the Consumer Protection Law and the Civil Law, only the provisions of the Consumer Protection Law will apply, and the application of the Civil Law will be excluded.

The Theory of Free Competition and Cooperation of Claims

It is believed that Article 7 of the Consumer Protection Law and Article 191-1 of the Civil Code still have different legal effects at the constitutive element level in terms of norms, and the victim should be allowed the opportunity to freely choose the right to claim. That is, these two articles are not mutually exclusive.

The Theory of Competition and Cooperation of Freedom of Request

It is believed that Article 7 of the Consumer Protection Law and Article 191-1 of the Civil Code can be claimed by both parties. According to the theory of the new litigation object, it should only be a method of attack and defense. And according to Article 199-1 of the Civil Procedure Law, if a party claims that the product is defective and causes damage, if he only claims the provisions of the Civil Law or the Consumer Protection Law, the court is obliged to clarify whether it intends to add the provisions of the Consumer Protection Law or the Civil Law Regulation. If the court does not clarify, it is a judgment in violation of the law.

4. Patient Safety Discussion

4.1. Patient Safety

Eysenbach and Diepgen pointed out in a paper published in 2001 that consumer health informatics and smart medicine will redefine health care in the 21st century and guide "evidence-based patient choice" (EBPC) development, which combines evidence-based medicine and patient-centered medicine. Wise Information Technology of Medicine can make clinical care safer and more efficient, but some scholars have raised safety warnings for smart medical applications at the public end. Coiera et al. pointed out that the "personally controlled digital health record" (PCEHR) has the potential risk of causing harm to patients, but there is a lack of national institutions to establish reference guidelines for the safety of smart medical applications. The Institute of Medicine (IOM) in the United States published a report on medical information technology and patient safety in 2012: "Health IT and Patient Safety: Building Safer Systems for Better Care", which pointed out that medical information technology caused Patient harm, although reported, is lacking in sufficient research evidence to quantify the extent of these harms. The report also suggested that the U.S. Department of Health should establish a new Health IT Safety Council to evaluate the criteria for monitoring "IT security" and "using IT to improve security", and suggested that FDA should specifically regulate the application of medical information technology. The existing laws on privacy protection cannot fully cover the application of Wise Information Technology of Medicine, which is also an important reason for experts and scholars to suggest that the government should strengthen supervision. However, although government intervention can reduce the possibility of harm to the public caused by smart medical applications, it may limit the innovation and development of technology.

4.2. Solution: Establishment of Supervision Sandbox System

Promoting financial technology (Fintech) in the financial field, perhaps "theregulatory sandbox" can provide an environment for the industry to develop innovative technologies and applications while taking into account the protection of the public's rights and interests. The supervision sandbox means that within a limited scope, companies can experiment with innovative solutions in a relatively relaxed legal environment, and test and verify the feasibility of their business models within a specific period. The Ministry of Health of Singapore announced the establishment of a supervision sandbox system for medical drugs and technology.

5. Black Box Problem Discussion

5.1. Black Box Problems Caused by Algorithms

Precision medicine and smart medicine are two different concepts. Precision medicine is to enhance the existing ability of doctors, while smart medicine is to reduce the labor of doctors. In recent years, medicine has gradually developed towards personalized medicine. In the past, drug treatment was still designed for ordinary patients. Such a one-size-fit-all treatment method may be very effective for some patients. However, based on the differences in each person's genes or other physiological factors, another group of patients may just suffer the side effects of treatment in vain, so precision medicine has emerged. According to the National Cancer Institute (NCI), precision medicine is defined as medicine that uses genetic information about individual diseases to guide its diagnosis or treatment.

The application of AI technology to the clinical aspects of precision medicine can optimize patient data through machine learning and deep learning algorithm analysis, so as to achieve early and accurate diagnosis, thereby reducing medical costs; in terms of drug research, AI algorithm Its computing power can accelerate the development of clinical precision medicine, so as to develop personalized drug design and provide personalized treatment plans, such as pharmacogenomics, which is representative of the application. According to the specific physiological index of the patient, and find the most suitable drug through genetic analysis. In addition, through the combination of AI machine learning algorithm and big data analysis to develop new drugs, strengthen computer-aided drug screening and design, shorten the time course of new drug development and increase the probability of success, it will help the research and development of personalized drugs, and AI medical realization Purpose of precision medicine. However, the AI medical system developed by machine learning algorithms inevitably has a black box problem, making it impossible for users of AI

medical applications to know the calculation process and influencing factors of medical judgments and decision results, and it may even be because the AI system involves business secrets. The refusal of the product manufacturer to disclose the details of the algorithm may also cause the doctor to use the AI system to be unable to inform the patient of the basis for judging the condition, and thus unable to fulfill the obligation of informing and consenting.

5.2. Solution: Formulation of Norms

Since algorithms are the key to intelligent medical computing decision-making, regarding the social inequality and discrimination caused by AI computing decision-making, based on social fairness, how should AI data controllers be required to act or how should relevant fields be established?, so as to improve inequality and safeguard the basic rights of human beings, is one of the directions that must be paid attention. Therefore, it is a good countermeasure to actively formulate appropriate norms.

6. Discussion of Privacy and Differential Treatment Issues

6.1. Privacy and Differential Treatment Caused by Biological Information

Medical records, surgery, and hospital care in medical institutions, as well as biological data such as specimens and genes, as well as labor health examination records and national health insurance records. Declaration documents, and wearable devices and medical mobile applications that record personal physiological status. The particularity of these data is that it is easy to reveal personal psychological or physical private information. For example, in the treatment reports on psychological medicine or sexually transmitted diseases, personal friendships may be disclosed; or medical images of health examinations may reveal general personal information. The most private parts of the body and diseases; for example, the health information disclosed by genetic information may affect personal employment, schooling, insurance, etc., resulting in privacy and differential treatment issues.

6.2. Solution: Specific Implementation of Personal Data Protection

Since the specific implementation of personal data protection is relatively important, this can be learned from the experience of other countries. Taking the European Union as an example, the European Union has taken the use of AI into consideration during the formulation of laws and regulations, and set four principles for personal data protection: the principle[1]of specific purpose, data minimization, transparency and accountability. Taking GDPR as an example, it is stated in Recital 71 that in order to ensure equal and transparent processing of data subjects, data controllers are required to take appropriate technical and technical measures in order to reduce the risk of related errors and prevent data based on race or Discrimination issues arising from sensitive information such as ethnic origin, political opinion, religion or belief, trade union membership, genetic or health status, etc. occur. It can be seen from this provision that the data controller must be required to properly control the factors that cause AI to produce biased data quality and algorithm design, so as to reduce the impact of biased factors and ensure the quality of the AI system. Regarding the issue of discrimination in the relevant AI application fields, some scholars also believe that the establishment of the Whistleblower Protection Law should be promoted so that whistleblowers can have proper protection when reporting AI violations of anti-discrimination laws in various fields, and further Implement the accountability of AI while preventing the social risks caused by the misuse of AI technology.

If GDPR is used as the basis for requiring data controllers and data processors to ensure information security, according to[2]the requirements of GDPR Article 32, they must implement appropriate technological and organized measures in accordance with relevant actual conditions such as technology and cost , such as using Encryption technologies such as pseudonymization of personal data ensure the continuous confidentiality, integrity, availability and flexibility of systems and services, and respond to the availability and usability of personal data in a timely manner after an accident occurs. At the same time, regular evaluation and testing are required, Measure and ensure the effectiveness of security measures.

[1]The discussion content of Prof. Chih-hsiung Thomas Chen's research team and the source of related reference materials on the Internet: https://www.inside.com.tw/article/23814-ai-privacy-medical .
[2]https://gdpr-info.eu/

GDPR Article 35[3]also stipulates that if the data controller or data processor needs to regularly and systematically monitor the parties on a large scale, or needs to process special data related to health or crime on a large scale, the data controller or data processor should designate A data protection officer with professional qualifications shall conduct an impact assessment of personal data protection before data processing, and if the assessment result finds that the data processing has not taken measures to reduce risks and there is a high risk, the data controller shall report to the data Consult regulatory authorities before handling. In addition, GDPR Article 42[4]also requires data controllers and data processors to comply with the relevant principles of data processing in GDPR, and must also be certified by the data protection certification mechanism to prove that they have provided appropriate protection measures, and the certification period it can only last for a maximum of 3 years.

7. A LARGE AMOUNT OF GENETIC INFORMATION REVEALS AND DISCUSSES ISSUES

7.1. Mass Disclosure of Genetic Information

Genetic information can be used to identify personal characteristics and for disease analysis, treatment, prescribing, or as the basis for fertility counseling, and is also seen as having great potential commercially. With the advancement of biomedical technology, even the genetic map of the entire family can be known from individual tiny genes. Coupled with the advancement of AI technology, the personal information that can be revealed by relying on AI calculations is beyond the imagination of ordinary people. So far, the privacy risks caused by AI medical care are not limited to individuals, but can also extend from personal data privacy risks to social impacts such as ethnic groups and races.

7.2. Solution: establishment of Information Security System

From the information security requirements of GDPR, we can see that in the face of security concerns caused by AI technology and big data, not only the information security standards that are flexible to the system specification are provided to deal with the information security problems faced by different fields , but also the information security issues faced by different fields. Security personnel also provide a considerable degree of management when dealing with sensitive data, and even set up an authentication mechanism to reduce information security risks brought about by the rapid update of AI and other related information and communication technologies. As for the countermeasures when personal data leaks occur, GDPR Article 33(1)[5]it requires data users to avoid undue delay and, if possible, notify the relevant supervisory authority within 72 hours of becoming aware of the incident. Those who fail to notify within the time must also explain the reasons when notifying. The data subject must also be notified when the leaked data poses a high risk to the rights of the data subject. Therefore, it can be seen that GDPR requires data users to perform various notification obligations, which is to protect the timely rescue of data leaks at the first time, reduce damage and protect the privacy of data subjects under the operation of AI technology. When the various AI devices and cloud data connected in series through the network are leaked , they can be discovered and notified in time to prevent the damage from expanding infinitely. Therefore, the establishment and maintenance of information security system is urgent.

7.3. Risks and Data Utilization of Wise Information Technology of Medicine

In order to prevent the risks caused by the misuse of artificial intelligence technology, through the discussion of related risk issues in Wise Information Technology of Medicine, we can start from the safety of different risk levels, carry out the development of software design and development life cycle , evaluate the possible risks and respond to them. . In addition, in order to achieve the data utilization promoted by Wise Information Technology of Medicine, it is necessary to consider both the protection of personal data and the full use of data.

8. RISK CLASSIFICATION

8.1. Major Risk Level

If a medical device software failure or potential defect may directly cause **serious injury to patients or users**, the medical device software belongs to the major risk level. If the failure or potential defect

[3]https://gdpr-info.eu/
[4]https://gdpr-info.eu/
[5]https://gdpr-info.eu/

of the medical device software causes incorrect or delayed information, which may indirectly cause **serious injury to the patient or user**, the medical device software also belongs to the major risk level.

8.2. Moderate Risk Level

If a medical device software failure or potential defect may directly cause **minor injury to patients or users**, the medical device software belongs to the moderate risk level. If the failure or potential defect of the medical device software causes incorrect or delayed information, which may indirectly cause **minor injury to the patient or user**, the medical device software also belongs to the moderate risk level.

8.3. Minor Risk Level

Minor risk level means that software failures or potential design defects of medical devices will not cause any harm to patients or users.

8.4. Different Levels of Security Control

Safety of Different Risk Levels

According to the different risk levels of medical device management, the information that manufacturers should submit and the level of detail are also different, but such information is generated in the process of medical device software design and development. Regardless of whether it should be submitted or not, medical device manufacturers should submit Establish, implement and maintain in accordance with relevant provisions of good manufacturing practices for medical devices.[6]

The current definition of "medical software" in Taiwan generally refers to processing software that collects, stores, analyzes, displays, and transforms human health status, physiological parameters, and medical-related records. The guidelines for medical software provide several types of software as examples of classification, but There are no clear examples in the artificial intelligence section, so the "Artificial Intelligence/Machine Learning Guidelines" is formulated to define artificial intelligence/machine learning-based software for medical devices (Artificial Intelligent/Machine Learning-Based Software as a Medical Device, AI/ML-Based SaMD) is a medical device software that uses clinical data (assay data, databases or images, etc.) as a source to make the program simulate human reasoning or autonomous learning through artificially designed software learning models or training methods, and then adjust its performance. The guideline mentions the key points of inspection, registration and review of medical device software with artificial intelligence/machine learning technology, and also applies to medical devices that use artificial intelligence/machine learning technology to provide part of function. However, the guidelines are not used to define the scope of medical equipment management and the determination of management levels. The principles for the scope of management of medical equipment software and the determination of classification and classification are the "Reference Guidelines for Classification and Grading of Medical Software" and "Measures for the Administration of Classification and Grading of Medical Devices".

Table1. *Life cycle data of medical device software design and development based on risk classification*

Medical device software design and development life cycle information	**Minor risk level (minor)**	**Moderate risk level (moderate)**	**Major risk level (major)**
Risk Level of Medical Device Software (Level of Concern)	All levels should be attached, explaining the process and results of determining the risk level of the medical device software.		
Description of Medical Equipment Software Description	All grades should be attached, summarizing the function and operating environment of the medical device software.		
Hazard Analysis of Medical Device Hazard Analysis	All grades should be attached, and the hazards, risk assessment and risk control methods related to medical device hardware and software should be explained in a tabular form.		

[6]The Ministry of Health (87) Health Department Announcement No. 87042470 of the Executive Yuan , the Ministry of Economic Affairs (87) Jinggong Zi Announcement No. 87260757 issued "Good Manufacturing Practice for Medical Devices"

Medical Equipment Software Requirements Specification, SRS	The summary describes the functional requirement specification of the medical device software.	Completely describe the required specifications of the medical device software.	
Medical equipment software (Architecture Design Chart)	No need to attach	The functional unit (Functional unit) and module (software modules) of the medical device software must be specified in detail, including state diagrams (state diagrams) and flow charts (flow charts).	
Medical Equipment Software Design Specification, SDS	No need to attach	Attached are the software design specifications for medical devices.	
Traceability Analysis	All grades should be attached with medical device software traceability analysis documents, including software requirements specification (SRS), software design specification (SDS), hazards (identified hazards), hazard reduction (mitigations), and verification and confirmation tests (verification and Validation testing) retrospective records.		
Medical Equipment Software Development Environment Description	No need to attach	Attached is a summary of the medical device software life cycle development plan, including a summary description of software configuration management and software maintenance activities.	Attach a summary of the medical device software life cycle development plan, including control documents generated during the development process, software configuration management plan and software maintenance plan documents. Attach the description of the control/baseline documents and software coding standards of the software development process.
Verification and Validation Documentation	Attached is the software function test plan (plan), test qualification criteria, and test result summary.	Describes verification and validation at the unit, integration, and system levels. Attached is the system-level test method (protocol), test qualification criteria, and test results.	Describes verification and validation at the unit, integration, and system levels. Attach unit, integration and system level test methods (protocol), test pass criteria, test results.
Revision Level History of Medical Device Software	Attach the historical records of medical device software revisions, including date, version number, changes between versions, and the final release version.		
Unresolved Anomalies (Bugs or Defects)	No need to attach	Attach a list of unresolved exceptions, the impact of these unresolved exceptions on product safety and effectiveness, including human factors engineering, etc.	

Source: *"Guidelines for Validation of Medical Device Software" issued by the Food and Drug Administration of the Ministry of Health and Welfare in 2017.*

Comparison of Wise Information Technology of Medicine Risk Classification in the European Union, the United States, and Taiwan

Taking the EU as an example, risks are defined and categorized in terms of unacceptable/ high/limited/minimum or no risk. Taking the United States again as an example, the Possible Framework for Risk Categorization is based on the importance of product information in medical decision-making (treatment or diagnosis, promoting clinical management, informing clinical management information), and applicable medical care situations (critical, serious, non-serious), and the degree of impact of the product on patients or public health is divided into four risk categories (category I, II, III, IV). The lowest impact is Class I products, which can be used to inform the clinical management information of serious and non-serious diseases, or promote the clinical management of non-serious diseases; conversely, the highest impact is Class IV products, which can provide the function of treating or diagnosing critical diseases. This risk classification is not intended to replace the current medical device classification system (Class 1, 2, 3), but to distinguish software product risk categories to provide risk consideration recommendations suitable for various software products. The European Union, the United States, and Taiwan's smart medical risk classification are compared in Table 2.

Table2. *Comparison of Wise Information Technology of Medicine risk categories in the EU, the US, and Taiwan*

	European Union (Categorize risk from high to low according to unacceptable/ high/ limited/ minimal or no risk definit ions)	**American SaMD (Categorized according to IV / III / II / I definition from high to low risk)**	**our country (Categorize risks from high to low according to major/ moderate/ minor definitions)**
Low	Allows free use of AI with minimal risk.	1. SaMD that provides information to drive clinical management of a disease or conditions in a non-serious situation or condition is a Category I and is considered to be of low impact. 2. SaMD that provides information to inform clinical management for a disease or conditions in a serious situation or condition is a Category I and is considered to be of low impact. 3. SaMD that provides information to inform clinical management for a disease or conditions in a non-serious situation or condition is a Category I and is considered to be of low impact.	If the software failure or latent defect of the medical device will not cause any harm to the patient or user.

Middle	AI with specific transparency obligations, such as when using AI, users should be aware that they are interacting with the machine so that they can make an informed decision to continue or opt out.	1. SaMD that provides information to treat or diagnose a disease or conditions in a nonserious situation or condition is a Category II and is considered to be of medium impact 2. SaMD that provides information to drive clinical management of a disease or conditions in a serious situation or condition is a Category II and is considered to be of medium impact. 3. SaMD that provides information to inform clinical management for a disease or conditions in a critical situation or condition is a Category II and is considered to be of medium impact.	If a medical device software failure or potential defect may directly cause minor injury to patients or users, the medical device software belongs to the medium risk level. If the failure or potential defect of the medical device software causes incorrect or delayed information, which may indirectly cause minor injury to the patient or user, the medical device software also belongs to the medium risk level.
Intermediate	High-risk AI must comply with strict obligations before it can be brought to the market, and such use must be authorized by a judicial or other independent authority and appropriately limited in terms of time, geographic scope, and searchable repositories.	1. SaMD that provides information to treat or diagnose a disease or conditions in a serious situation or condition is a Category III and is considered to be of high impact. 2. SaMD that provides information to drive clinical management of a disease or conditions in a critical situation or condition is a Category III and is considered to be of high impact.	none
High	Anything deemed to pose a clear threat to people's safety, livelihood, rights is prohibited.	SaMD that provides information to treat or diagnose a disease or conditions in a critical situation or condition is a Category IV and is considered to be of very high impact.	If a medical device software failure or potential defect may directly cause serious injury to patients or users, the medical device software belongs to the major risk level. If the failure or potential defect of the medical device software causes incorrect or delayed information, which may indirectly cause serious injury to the patient or user, the medical device software also belongs to the major risk level.

Source: *Discussion by Professor Prof. Chih-hsiung Thomas Chen's research team.*

In addition, the US FDA announced a "Software as a Medical Device (SaMD): Clinical Evaluation" guideline in December 2017, which was directly imported into the regulatory document issued by IMDRF in September of the same year (IMDRF/SaMD WG/N41Final:2017) , this document recommends that medical device software manufacturers conduct a complete clinical evaluation (clinical evaluation) before the product goes on the market, by continuously generating, collecting, analyzing and evaluating clinical data, and then generating clinical evidence to verify that the product is sufficiently safe and effective sex, and can meet its declared efficacy. The clinical assessment of SaMD recommended by the guidelines can be divided into the following two steps:

First, Valid Clinical Association

Should be confirmed whether the output information of SaMD can accurately correspond to the medical conditions for which it is declared applicable. Effective clinical relevance can be considered as an indicator of clinical acceptability and represents how clinically meaningful and confident the output information of the SaMD is in its declared intended use.

Second, Technical Validation

Should be confirmed whether SaMD is constructed correctly, including whether it can process input data stably and produce correct and accurate output results with repeatability and reproducibility.

The Application of Data for the Promotion of Intelligent Medical Care

At present, Taiwan may learn from the experience of other countries in the use of data , such as EHDS, GDPR, etc.

The European Health Data Space (EHDS)

The European Health Data Space (EHDS) is one of the 10 strategic fields proposed in The European data strategy, the purpose is to build on the framework of the Data Act and the Data Governance Act, establish a single data market in Europe, and improve the transmission and availability of health data. This proposal for the use of electronic health data can be divided into the following two parts:

Primary Use

For the rights enshrined in the EU General Data Protection Regulation (GDPR), supplementary supporting protection mechanisms are added, and the obligations of medical personnel and other health practitioners against EHDS are established. According to the provisions of EHDS Article 3, data subjects can obtain their own electronic health information immediately and free of charge, and can also change electronic health information online, strengthening the right to data sharing and portability among member states. In addition, EHDS also designated MyHealth@EU as a common platform to strengthen the transmission of electronic health data across borders, so that data subjects can more easily grasp their electronic health data.

Secondary Use

Use the data for research, innovation, policy development, patient safety or regulatory activities. Chapter IV defines a set of data types, regulates the established purposes that can be used and the prohibited purposes (such as commercial advertising, increasing insurance, developing dangerous products), and stipulates that member states must establish a health data access body (health data access body)), so as to facilitate the secondary use of electronic health data and ensure that electronic data generated by data holders (data holders) can be provided to data users.

Member states should establish penalties to implement the EHDS norms, and also establish the European Health Data Space Board (EHDS Board) to promote digital health authorities and health access data bodies The cooperation between, especially the relationship between primary and secondary use of electronic health data, as well as the relevant regulations of the joint control groups for EU infrastructure, whose task is to discuss the primary and secondary use of electronic health data Make relevant decisions on the cross-border digital infrastructure required for secondary use.

The General Data Protection Regulation (GDPR)

Referring to the EU GDPR, the United States initially introduced the first and most comprehensive data protection act from California (California Consumer Privacy Act of 2018, CCPA). Japan

promulgated the Act on the Protection of Personal Information (APPI) in 2003, which was implemented in 2005. Although Article 28 of the Act gives data subjects the right to request information disclosure, there is no provision for data portability rights clause. The Personal Information Protection Commission (The Personal Information Protection Commission) and scholars suggested that in addition to moving towards the legislative content of GDPR and expanding the right to data disclosure, they also mentioned that the right to data portability must be in specific areas (such as : Financial and medical) legislation and must understand that the right to data portability is not limited to personal data protection, but also related to industrial development and competition policies.

Basis of Claims, Exclusionary Application Circumstances

Claim Basis: Provisions in Section 2 of Section 1798.130 Section a.

The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.

Exclusion Range

This act shall not apply to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act (Part 2.6 commencing with Section 56 of Division 1) or governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996. For purposes of this subdivision, the definition of “medical information” in Section 56.05 shall apply and the definitions of “protected health information” and “covered entity” from the federal privacy rule shall apply.

Circumstances that May Apply

Additionally, these exclusions need to be reviewed carefully as they may not cover all medical information a business might collect. For example, when applying safety measures for COVID-19, medical information collected from employees and others may not fall under the definition of “med information” under the CMIA or “protected health information” under HIPAA.

9. CONCLUSION

This article is a preliminary view, and I hope to use it as an inspiration to stimulate more discussions and in-depth discussions. In order to make readers more clear about the focus of this article, the accountabilities and risk assessments of Taiwan's Wise Information Technology of Medicine are summarized in Table 3.

Table3. *Accountabilities and risk assessment of Wise Information Technology of Medicine in Taiwan*

Accountabilities of Wise Information Technology of Medicine	**Risk Assessment of Wise Information Technology of Medicine**
●product liability ➢Adopt "no-fault liability" for business operators; adopt "presumed liability for negligence" for the production, manufacturing or processing, and design of commodities. ➢Solution: Discussion on legal protection and legal competition (including competition and cooperation between consumer protection law, civil law and Pharmaceutical Affairs Act, and competition and cooperation between civil law	●Risk classification ➢Major Risk Level ➢medium risk level ➢Minor Risk Level ●Different levels of security control ➢Different grades of security ➢Comparison of Risk Classification of Wise Information Technology of Medicine in the European Union, the United States, and Taiwan ●The application of data for the promotion of Wise

and consumer protection law) ●patient safety ➢Potential risk of patient harm from Personally Controlled Digital Health Record (PCEHR) ➢Solution: Establishment of supervision sandbox system ●black box problem ➢AI medical systems developed by machine learning algorithms inevitably have black box problems ➢Solution: Formulation of norms ●Privacy and Differential Treatment ➢Issues of Privacy and Differential Treatment Caused by Bioinformatics ➢Solution: concrete implementation of personal data protection ●A large amount of genetic information is revealed ➢Privacy Risk Issues of Gene Information Disclosure ➢Solution: Establishment of information security system	Information Technology of Medicine (learning from the experience of other countries) ➢The European Health Data Space, EHDS (including Primary useandSecondary use) ➢EU GDPR ➢Basis of Claims, Exclusions and Possible Applicability

Source: *Author's self-made.*

REFERENCES

Chen Millingxiong(2021), ***Smart Healthcare and Law***, Hanlu Books.

Focualt, M. 1975, Surveilier et Punir.

Food and Drug Administration of the Ministry of Health and Welfare (2017),***Guidelines for Validation of Medical Device Software***, Taiwan (R. O. C.).

Lin Wenyuan**,**https://case.ntu.edu.tw/blog/?p=37579.

Liu Jingyi, ***artificial intelligence governance in the eyes of legal people--- what kind of concept is --- citizen in the AI era***, https://tw.news.yahoo.com/news/070605399.html

Liu Juncheng, Luo Mingjian, and Naineng Intelligent Co., Ltd., eds. (2021), ***Understanding Artificial Intelligence --- the Fourth Wave of Industrial Revolution***, All China Books.

Shah, Jugar. (2019). "Performance tuning of SQL Server with AWS Machine Learning." ***AWS***, October 6 interview quoted from Wenyuan Lin**,** https://case.ntu.edu.tw/blog/?p=37579.

Teare , HJ, Prictor , M. and Kaye, J. (2021). Reflections on Dynamic Consent in Biomedical Research: Stories So Far. ***European Journal of Human Genetics***, 29(4), 649-656.

The content of Professor Peng Senming's speech.

The Ministry of Health (87) Health Department Announcement No. 87042470 of the Executive Yuan , the Ministry of Economic Affairs (87) Jinggong Zi Announcement No. 87260757 issued "Good Manufacturing Practice for Medical Devices".

XieZhengxun, Liao Juezhou, Li Lianwang, eds. (2021), ***Artificial Intelligence: Introduction to Intelligent Systems*** (Third Edition), Quanhua Books.

Xinxi Chen, Dawei Guo, and Jie Li, eds. (2021), ***Introduction to Artificial Intelligence***(First Edition Four Brushes), Hon Hai Education Foundation.

Yuzhen Ding and Zilun Lin (2020), Discussion on the Application Potential of Artificial Intelligence to Improve Government Public Governance, ***Archives Semi-Annual Journal***, Vol. 19, No. 2, pp. 24-41.

ZHANG Zhiyong, LIAO Wenhua, SHI Guiping,WANG Shengshi, You Guozhong, ed. (2021), ***AI Artificial Intelligence*** (Second Edition), Quanhua Books.

https://gdpr-info.eu/

https://medium.com/

https://zh.wikipedia.org/zh-tw

https://zh.m.wikipedia.org/zh-tw/

https://smart.huanqiu.com/article/9CaKrnK99ND

http://www.worldpeoplenews.com/content/news/319606

https://global.udn.com/global_vision/story/8662/5803237
https://www.thinkhk.com/article/2018-06/21/27646.html
https://www.inside.com.tw/article/23814-ai-privacy-medical
https://www.bnext.com.tw/article/41534/3-key-techniques-of-ai ?
https://www.inside.com.tw/article/15033-tsmc-president-apec-ai
https://www.bnext.com.tw/article/71939/data-governance-how-to
https://edge.aif.tw/eric-huang-column-uncanny-valley/
https://ai.iias.sinica.edu.tw/how-to-create-common-good-in-society-with-ai/
https://www.charmingscitech.nat.gov.tw/post/perspective2-smartcity
https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd
https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=e127c0b0-9bc2-470d-ab47-404d877e64cf
https://official.kaijui-tech.com/what-is-the-impact-of-artificial-intelligence-ai-on-society/

AUTHOR'S BIOGRAPHY

Former researcher at National Yang Ming Chiao Tung University, currently seconded to National Taiwan Normal University. Served at National Taiwan University and Tsing Hua University. Passionate about academic research and research interests are mainly in issues related to emerging technologies. Besides, the author is also a adjunct associate professor. It also has a good reputation in teaching, guide students to think with heuristic teaching.

Citation: *Wen-Chuan Ke. "A Preliminary Study on the Accountabilities and Risks of Wise Information Technology of Medicine in Taiwan" International Journal of Humanities Social Sciences and Education (IJHSSE), vol 11, no. 4, 2024, pp. 47-60. DOI:* https://doi.org/*10.20431/2349- 0381.1104004.*