Assessment3

Task 2

Ting Wang-Student ID: 52094016

Subtask2.1

To deploy AI to the medical field, we need to understand the government's regulatory framework. AI in healthcare must meet the following rules:

ICO UK AI document:

Protect users' rights and freedoms from high risks, protect user privacy, and at the same time protect user data portability rights.

Comply with the principles of legality, fairness and transparency, ensure the accuracy of statistical data, and fully respond to risks of bias and discrimination.

Thoroughly evaluate the security of artificial intelligence systems, prevent security accidents from occurring, and respond to potential security risks caused by software vulnerabilities on time.

Perform a data protection impact assessment. The data processing process must be entirely legal, increase the richness of the data, meet the user's expectations for processing, and identify and evaluate data risks.

EC's AI framework:

The European EC's AI white paper elaborates on the regulatory framework for artificial intelligence and mainly puts forward seven requirements: human institutions and supervision; technological robustness and security; privacy and data processing; transparency; diversity, non-discrimination and fairness; society environmental well-being; accountability. The white paper pointed out that the main risks associated with artificial intelligence involve rules intended to protect fundamental rights and security issues and reliability-related issues.

FDA AI Healthcare:

FDA expects manufacturers to obtain the promise of transparency and real-world performance of AI/ML-based medical device software. The regulatory framework of "pre-specification" and "algorithm change protocol" enables the iterative improvement capabilities of AI/ML medical device software to be within the scope of FDA supervision, ensuring patient safety.

Establish quality system and good ML operating procedures

Preliminary guarantee for the safety and effectiveness of AI/ML-based medical device software before market launch

Companies are expected to monitor AI/ML devices to develop, verify, and execute algorithm changes.

Use post-marketing real-world performance reports to continuously improve the transparency of the software to users and the FDA.

Subtask2.2

Frameworks	References	Individual Requirements	Technical Solutions
ICO UK's AI documents	Protect users' personal rights and freedom from high risks	Fully protect the rights and interests of users. Protect users' right to know, correction, data transfer, etc.	Company should take measures to protect the rights, freedoms and legitimate interests of individuals. For example, a company can provide public information explaining where the data was obtained to train an artificial intelligence system.
	Observe the principles of lawfulness, fairness and transparency	The AI application may lead to unfair and illegal use of data	To ensure that the AI system is statistically accurate enough to ensure that the personal data it processes comply with the principle of fairness, the collection of complete data sets needs to be rich, correct, and large. Before training the model, fully analyze the data set, eliminate bias, conduct robust testing of any anti-discrimination measures, and monitor the performance of ML system continuously.1
	Fully evaluate the security of the artificial intelligence system to ensure that the data is minimized	Prevent unauthorized or illegal processing, accidental loss, destruction or damage. Software vulnerabilities may lead to information leakage and even medical accidents	Separate the ML development environment from other IT infrastructure as much as possible. Timely deal with software vulnerabilities caused by introducing new AI-related code and infrastructure. To reduce the risk of being attacked, developers can monitor queries from API users to detect whether they are being used suspiciously. Regular testing, evaluation, and establishment of a complete model testing process. Use disturb or add "noise"; and joint learning methods to protect privacy.2
	Conduct DPIA	Avoid illegal use of data, AI may bring harm to the potential impact on individuals.	In DPIA, we need to evaluate how to collect, store and use data; the amount and diversity of data; the nature of relationship with individuals; and the intended outcomes for individuals.

Frameworks	References	Individual Requirements	Technical Solutions
FDA's AI Healthcare	Establish quality system and good ML operating procedures	Users may worry that the performance of the AI system may decline after use, causing accidents, or that the AI system's lifecycle may be short.	For the development, delivery and maintenance of AI systems throughout the life cycle, high-quality products that comply with corresponding standards and regulations
	Preliminary guarantee for the safety and effectiveness of AI/ML-based medical device software before market launch	Individuals have doubts about the security of the AI system	Prove reasonable assurance of its safety and effectiveness, and establish clear expectations for AI/ML-based medical device software to continuously manage patient risks throughout the life cycle.
	Manufacturers are expected to monitor AI/ML devices as they develop, verify, and execute algorithm changes	The behavior of AI products may be uncontrollable, and the public expects to strengthen supervision.	Developers should analyze possible risks and incorporate risk management methods, while protecting the individual’s right to know
	Manufacturers are expected to monitor AI/ML devices as they develop, verify, and execute algorithm changes	Due to the black box nature of AI, users are hard to know performance of AI	Continue to evaluate AI performance for different groups of people, maintain product safety and effectiveness, and increase user trust

Frameworks	References	Individual Requirements	Technical Solutions
EC's AI framework	Human institutions and supervision	Ensure that medical AI is reviewed before listing and establish clear expectations	Ensure that when AI makes major determinations, it is made under appropriate human supervision and compliance with GDPR regulations.
	Technical robustness and safety	AI system life cycle stages should be robust, accurate, and the results are repeatable	Appropriately consider the risks that they may generate in advance and make a risk assessment. Ensure that the artificial intelligence system can withstand open attacks and more subtle attempts to manipulate data or the algorithm itself, and take mitigation measures.
	Privacy and personal data processing	The use of AI may infringe on the values of the European Union. Users worry that AI may bring influence and discrimination. There is no similar social control mechanism to control human behavior.	privacy： Discussed above Personal information： Discussed above
	transparency	Ensure data transparency	Discussed above
	Diversity, non-discrimination and fairness	AI and developers should be bound by European law on fundamental rights, consumer protection, and product safety and liability rules	Discussed above

Frameworks	References	Individual Requirements	Technical Solutions
	Social and environmental well-being	AI should be critically examined and trained to make choices that are beneficial to patients	Ensure the checkability of the model and make efforts for public health.
	Accountability	AI embedded products and services may bring security risks to individuals, and users hope to have a good responsibility tracking mechanism	Improve the company's accountability mechanism and self-inspection mechanism, refine the model development and deployment process, and facilitate the accountability of problems.

- **Main body of the article word count: 1088**

Resources: