**Data Science and AI Module – Continuous Assessment 2023(100%)**

**BSc (Hons) Applied Computing Yr4 & BSc (Hons) Computing Yr4**

# Question 1: What issues for potential bias/ethical questions exist with AI Medical Doctor? (20%)

Answer:

Among the legal and ethical issues that artificial intelligence (AI) has brought to society, the importance of human perception is a key philosophical subject, along with privacy and monitoring, bias or intolerance. Modern digital technologies' arrival has sparked concerns that they could end up being a possible cause of inaccuracy and data breachesIn the healthcare sector, failures in procedure or protocol can have serious consequences for the patient who face those failure. It is crucial to remember that patients engage with doctors when they are at their most vulnerable. There must currently be clear policies in place to address any ethical and legal issues that may arise from the application of AI in medical settings. With a focus on the importance of algorithmic accessibility, privacy, and safety for all associated beneficiaries as well as the cybersecurity of related weaknesses, this analysis aims to address these pressing issues. (Stephenson et al. 2021).

## Applications of AI for Health Research

Using data generated for digital health records is a crucial component of AI-based health research (EHR). It may be challenging to utilize such data if the underlying database and information technology system does not control the spread of diverse or low-quality data. Yet, digitalized medical records can be improved using AI for research, quality control, and better clinical treatment. AI that has been effectively created and taught with enough data can help with identifying clinical best practices from electronic health records before going through the conventional route of scientific publication, guideline creation, and medical support tools. AI can help create new clinical practice models of healthcare delivery by studying clinical practice trends revealed in electronic medical records. (Stephenson et al. 2021).

## Artificial Intelligence in Drug Development:

In the future, it's expected that AI will accelerate and streamline the pharmaceutical manufacturing process. AI can change the labor- and resource-intensive drug development process into one that is data and resource-intensive by using robots and modeling genetic targets, drugs, tissues, diseases and their treatments, and pharmacokinetics. Artificial intelligence can speed up, make drug research more economical, and make it more effective (AI). Although, as with any pharmaceutical study, finding ensure the formulation of a secure and effective medication, AI has already been used to uncover potential Ebola virus medicines (Stephenson et al. 2021).

## Ethical Challenges:

It is always being debated whether AI "fits within known legal categories or if a new category with its own features and repercussions should arise." Although using AI in medical settings has a lot of potential to improve healthcare, it also presents ethical questions that we need to address right away. There are four major ethical issues must be resolved for medical AI to fully realise its potential: Informed consent to use data, protection and accessibility, algorithmic fairness and biases, and data privacy are all crucial considerations ( Gerke et al. 2020). In addition to being legally debatable, the legality of AI systems is also politically divisive. (Rodrigues et al. 2020)

## Global Legislations:

The study that formed the basis for the resolution was commissioned, managed, and published by the policy division for "Citizens' Rights and Constitutional Problems" in in response to an inquiry from the Committee on Legal Affairs of the European Parliament. The study emphasises the significance of a resolution calling for the swift creation of a legal framework for robots and AI that can anticipate and adapt to any medium-term technological breakthroughs (Albrecht et al 2022).

**Who Is Responsible for This?**

Unlike to doctors, technologists are not compelled by law to be held accountable for their actions; instead, in this sector, ethical standards of practise are followed. This comparison can be used to summarise the debate about whether technologists should be held accountable if AIS is applied in a healthcare setting and has a negative impact on patients. If a physician uses that data, they will not be able to adequately justify their choices if they are unable to account for the result of the AIS they are utilising. This absence of accountability raises concerns about the possible safety effects of using unverified or untestable AISs in medical settings. Several examples illustrate how each stakeholder is impacted by opacity (Smith et al 2020). The elements that need to be considered in order to make conceptual and methodological advancements for the moral assessment of machine learning-based healthcare research. Undoubtedly, that is a challenging aspect of technology. The decision on whether to use AI systems ultimately remains with the practitioners and hospitals that will be using them, despite the fact that we think a new structure and technique are needed for their approval. (Char et al. 2020)

Instead of replacing doctors and nurses, AI-powered medical devices will only make it simpler for them to decide how to administer treatments and operations. The top authorities of policymakers must develop a comprehensive framework because there is a dearth of research in this field. (Henz et al. 2021).

**Bias in AI Application:**

There is evidence that AI algorithms can incorporate and make extensive use of human and social biases. Yet, it is more appropriate to hold the underlying data accountable than the algorithm itself. Better AI algorithms can be created using data that includes human judgements or data that shows the second-order impacts of historical or cultural injustices. (Nelson et al. 2019) The processes used to gather and evaluate data can also introduce bias. User-generated data has the potential to serve as a feedback loop and create bias. To the extent that we know, there aren't any guidelines or standards for summarising and contrasting these models, but future work ought to take this into consideration to assist doctors and researchers. (Shah et al. 2020).

AI is transitioning from a "nice-to-have" to a necessary element of modern digital systems. As we start to rely more and more on AI for decision-making, it is crucial to ensure that judgements are made responsibly and without unfair biases. We believe that responsible, open, and accountable AI systems are necessary. Artificial intelligence (AI) algorithms are being utilised more frequently to improve patient outcomes and surgical outcomes, often exceeding people. Starting with limited applications, it may either replace present systems in the healthcare industry or coexist with them. It can be deemed unethical and unscientific to not use AI. (Parikh et al. 2019).

# Question 2: Outline a governance strategy for your chosen AI Medical Doctor?

# Answer :

Developing a governance strategy for an AI Medical Doctor involves defining the roles, responsibilities, and policies for its development, deployment, and ongoing operation. Here are some key elements that should be considered when outlining a governance strategy:

## Ethical Framework:

Define the ethical framework that governs the AI Medical Doctor, including the values and principles that underpin its development and deployment. This framework should address ethical issues related to data privacy, transparency, accountability, and fairness. This framework should be aligned with the organization's values and should be transparently communicated to stakeholders, including developers, data scientists, regulators, and users. (Reddy et al. 2019)

Certainly, here are some additional details on developing an ethical framework for an AI Medical Doctor, with relevant evidence and references:

### **Addressing data privacy:**

When creating an AI Medical Doctor, data privacy is a crucial ethical factor. Issues like informed consent, data anonymization, and data access controls should be covered by the framework. To protect patients' psychological well-being and reputations from privacy violations, AI systems should be secured, and patients' data must have their explicit agreement before it can be utilised for any purpose. Regulations that address data privacy in healthcare include the Health Insurance Portability and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in the EU. Following these rules can help guarantee that the AI Medical Doctor operates in an ethical and legal manner (Reddy et al. 2019).

### Ensuring transparency:

Transparency is another important ethical consideration when developing an AI Medical Doctor. The framework should address issues such as how the system makes decisions and how it handles errors or exceptions. This can help ensure that the system is accountable and that users have a clear understanding of how the system works. The AI Transparency Institute has developed a set of guidelines for transparency in AI systems. (Reddy et al. 2019)

### Addressing bias and fairness:

AI bais is another crucial ethical factor to take into account while creating an AI medical doctor.The framework should cover topics including how the system detects bias, how it lessens it, and how it ensures decision-making is fair. Substantial contribution of health-related or other data is necessary for the training of AI models. It was stated as "baises in, baises out" in the context of an AI model. Such biases might appear when the data used for training the AI models are insufficient or incomplete, or when they are not representative of the population being targeted. Due to societal prejudice (low access to healthcare) and comparatively small samples (minority groups), unrepresentative data can develop and worsen health inequalities. AI biased algorithms in the medical field could cause some patient populations risks to be under – or over-estimated. Of course, bias is a complicated concept, and humans too have baises. Nonetheless, it might be possible – and ethically necessary – to create AI systems that work to counteract human prejudices and produce more equitable, if still flawed, results (Reddy et al. 2019)

Hence Overall, developing an ethical framework for an AI Medical Doctor involves considering a range of ethical considerations relevant to AI and healthcare, and ensuring that the framework aligns with regulatory requirements and best practices in the field. By adhering to these considerations, organizations can help ensure that their AI Medical Doctor is ethical, transparent, and fair.

1. Governance Structure:

Define the governance structure for the AI Medical Doctor, including the roles and responsibilities of key stakeholders such as developers, data scientists, regulators, and users. This should include clear lines of accountability and decision-making processes. For example, a governance board or committee can be established to oversee the development and deployment of the AI Medical Doctor, with representatives from different stakeholder groups. The governance structure should also define the mechanisms for resolving disputes or conflicts that may arise among stakeholders (LaRosa et al. 2018).

### Defining roles and responsibilities:

Developing a governance structure for an AI Medical Doctor involves defining the roles and responsibilities of various stakeholders. This includes identifying who is responsible for the development, testing, and deployment of the system, as well as who is responsible for monitoring and evaluating its performance (LaRosa et al. 2018).

### Ensuring accountability:

Accountability is a critical component of any governance structure for an AI Medical Doctor. This involves establishing processes for identifying and addressing errors, omissions, and other issues that may arise during the development and use of the system (LaRosa et al. 2018).

### Implementing monitoring and evaluation:

Monitoring and evaluation are essential components of a governance structure for an AI Medical Doctor. This involves tracking the performance of the system over time and evaluating its impact on patients, healthcare providers, and other stakeholders (LoRosa et al. 2018).

### Addressing legal and regulatory issues:

Developing a governance structure for an AI Medical Doctor also involves addressing legal and regulatory issues. This includes ensuring compliance with relevant laws and regulations, as well as identifying and addressing any potential legal or regulatory challenges that may arise during the development and use of the system (LoRosa et al. 2018).

## Data Management:

Establish clear policies for data collection, storage, and usage. This should include data privacy and security measures that protect sensitive information. The data management policies should comply with regulatory requirements, such as HIPAA in the US. The policies should also address issues related to data quality, including data cleaning, normalization, and validation (Ruda et al. 2021).

### Validation and Testing:

Define validation and testing protocols to ensure that the AI Medical Doctor is functioning as intended and producing accurate results. This should include regular audits and reviews to ensure ongoing compliance with regulatory requirements. The validation and testing protocols should be designed to identify potential biases, errors, or other issues that may impact the accuracy and reliability of the AI Medical Doctor (Ruda et al. 2021).By implementing these elements, a governance strategy can provide a robust framework for the development and deployment of an AI Medical Doctor that aligns with ethical, legal, and regulatory requirements and promotes trust and transparency with stakeholders.

# Question 3: What Data Protection/Privacy issues exist for AI Medical Doctor?, if there are none then justify. (15%)

## Answer:

AI Medical Doctor systems can pose various data protection and privacy issues, including:

## Patient data privacy:

Many sensitive patient data sets, including medical records, genetic data, and biometric data, may be gathered and processed as a result of the use of AI Medical Doctor systems. To preserve patient privacy, the storage and processing of this data must adhere to data protection laws including GDPR and HIPAA. In recent years, data breaches in healthcare settings have increased, with the bulk of these breaches involving hacking and IT events, according to a research by the World Health Organization (WHO) (Liu et al. 2016).

In terms of patient data security, the use of AI Medical Doctor systems can pose several data protection and privacy issues, including:

### Unauthorized access:

AI Medical Doctor systems may be susceptible to unauthorised access by  outsiders, employees, hackers or third-party service providers. Patient data may be stolen, altered, or destroyed as a result of unauthorized access, which might have serious ramifications for patient privacy and healthcare results. Healthcare institutions must make sure that only authorised people may access patient data and that the data is encrypted, anonymized, or pseudonymized as necessary. (Kaissis et al. 2020).

### Transparency:

It's possible that patients are unaware of how AI Medical Doctor systems collect and use their data. Patients must be fully informed about how their data is gathered, processed, and used by healthcare organizations, especially when it comes to the usage of AI Medical Doctor systems. (Richardson et al. 2021).

### Accuracy and bias:

AI medical doctor systems must be accurate and reliable in order to avoid making prejudiced or incorrect judgements on patient treatment. Healthcare institutions must ensure that the data used to create and maintain AI Medical Doctor system is accurate and unbiased. (Richardson et al. 2021).

## Informed consent:

The obtaining of informed consent from patients is a crucial component of ethical AI Medical Doctor system. Patients need to be made aware of the types of data being gathered, how they will be utilised, and the advantages and disadvantages of employing AI in healthcare. In a study that was published in the Journal of Medical Ethics, Researchers discovered that patients were happy to submit their data with AI Medical Doctor system as long as patients were told about how their data will be used and given the choice to opt-out (Taitingfong et al. 2021).

The following are some specific patient data protection and privacy issues related to informed consent that can arise from the use of AI Medical Doctor systems:

### Lack of transparency:

Patients may not fully understand how their data will be used by AI Medical Doctor systems. Healthcare organizations must ensure that patients are adequately informed about the collection, processing, and use of their data, including how AI Medical Doctor systems are being used(Kaissis et al. 2020).

### Complex algorithms:

AI Medical Doctor systems may use complex algorithms to make decisions about patient care. Patients may not fully understand how these algorithms work or how they impact their care. Healthcare organizations must ensure that patients are informed about how these algorithms work and how they are used in decision-making (Kaissis et al. 2020).

## Bias in AI for data protection/ privacy:

Inaccurate diagnoses and treatment suggestions can result from bias in the AI medical doctor system, which can also serve to maintain current healthcare disparities. For instance, a study that appeared in the New England Journal of Medicine revealed that an AI Medical Doctor system that forecasts patient’s healthcare needs significantly underestimated the needs of black patients in comparison to those of white patients. By making sure that the data sets used to train the AI Medical Doctor system are representative and diverse, and that the algorithms used to analyse the data are accessible and auditable, this bias can be reduced. (Scheibner et al. 2021).

## Data breaches:

The use of AI Medical Doctor systems also poses a risk of data breaches, which can lead to the exposure of sensitive patient information. According to a report “Cost of data breach 2022” conduct by Ponemon Institute and analyzed and sponsored by the IBM, healthcare organizations face an average cost of $10.10 million for a data breach (IBM, 2022). This result in damage to reputation, loss of patient trust, and legal consequences. To mitigate this risk, healthcare organizations must invest in robust cybersecurity measures such as encryption and multi-factor authentication (Taitingfong et al. 2020).

### Cybersecurity vulnerabilities:

AI Medical Doctors may be exposed to cybersecurity dangers such malware, phishing scams, and hacking. These flaws could be used to access patient data without authorization, resulting in a data breach (Taitingfong et al. 2020).

### Insider threats:

Insiders with access to view patient data who are not allowed to do so can also be the source of data breaches. These insiders may improperly access or distribute patient data, either purposefully or accidentally, leading to a data breach (Taitingfong et al. 2020).

### Third-party risks:

In order to manage patient data, AI Medical Doctor systems may lean on other vendors or service providers. These outside parties could not follow the same level of privacy and data protection regulations as the healthcare business, which leaves them open to data breaches (Taitingfong et al. 2020).

### Regulatory and reputational risks:

Healthcare firms may suffer regulatory sanctions and reputational harm as a result of data breaches. If patients' data is exposed, the healthcare organization may lose their trust, which could result in a decline in sales and income. (Taitingfong et al. 2020).

### Legal consequences:

Legal repercussions, including litigation and liability claims, may result from data breaches. Healthcare businesses may be sued by patients for losses brought on by data breaches, including identity theft, monetary losses, and psychological suffering (Taitingfong et al. 2020).

# Reference

### Reference question 1

Stephenson J. “Who offers guidance on use of Artificial Intelligence in medicine.”, source: <https://jamanetwork.com/journals/jama-health-forum/fullarticle/2782125> , [ accessed: 13 july 2021].

Gerke S, Minssen T, Cohen G., “Ethical and legal challenges of artificial intelligence-driven healthcare.”, source: 10.1016/B978-0-12-818438-7.00012-5 , [accessed: 26 June 2020 ]

Rodrigues R., “Legal and human rights issues of AI: gaps, challenges and vulnerabilities.”,  [accessed:December ,2020] source: <https://www.sciencedirect.com/science/article/pii/S2666659620300056>

Jan Philipp Albrochet, “Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Europarleuropaeu”. source: <https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html> , [accessed February 3, 2022].

Nithesh Naik, B. M. Zeeshan Hameed, Dasharathraj K. Shetty, Dishant Swain, Milap Shah, Rahul Paul, Kaivalya Aggarwal, Sufyan Ibrahim, Vathsala Patil, Komal Smriti, Suyog Shetty, Bhavan Prasad Rai, Piotr Chlosta and Bhaskar K. Somani ,“Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?”,

<https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full> 14 March 2022

Shah M, Naik N, Somani BK, Hameed BMZ. Artificial Intelligence (AI) in urology-current use and future directions: an itrue study, source: <https://pubmed.ncbi.nlm.nih.gov/32479253/> , [accessed: 2020 May 27]

Helen Smith Clinical AI: opacity, accountability, responsibility and liability [2020]. source: <https://link.springer.com/article/10.1007/s00146-020-01019-6>

Char DS, Abràmoff MD, Feudtner C. Identifying ethical considerations for Machine Learning Healthcare Applications. [20-Nov-2020], source: <https://pubmed.ncbi.nlm.nih.gov/33103967/>

Patrick Henz, “Ethical and legal responsibility for artificial intelligence”, [September, 2021] source: 10.1007/s44163-021-00002-4

Nelson GS., “Bias in artificial intelligence”, source: <https://ncmedicaljournal.com/article/55108>, [accessed: july 01, 2019]

Parikh RB, Teeple S, Navathe AS, “Addressing bias in artificial intelligence in Health Care” , source: <https://jamanetwork.com/journals/jama/article-abstract/2756196> ,  [accessed: 22 November 2019]

### Reference question 2

Sandeep Reddy, Sonia Allan, Simon Coghlan, Paul Cooper , “A governance model for the application of AI in health care”, source <https://doi.org/10.1093/jamia/ocz192> , [accessed:4 nov 2019]

LaRosa Emily, Danks David, “Impacts on Trust on Healthcare Al” , source: <https://dl.acm.org/doi/pdf/10.1145/3278721.3278771> , [accessed: 2-Feb-2018]

kyarash shahriari, mana shahriari IEEE, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, source: [https://ieeexplore.ie ee.org/document/8058187](https://ieeexplore.ieee.org/document/8058187) , [accessed: 22-july 2017]

Roxana Radu, “Steering the governance of artificial intelligence: national strategies in perspective”, source:https://doi.org/10.1080/14494035.2021.1929728 , [accessed: 1-06-2021]

### Reference question 3:

Sharon Bassan, “Data privacy considerations for telehealth consumers amid COVID-19”, source: <https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsaa075/5905251> , [accessed: 2020-07-25]

Xiaoping Liu, XIAO-BAI LI, LUVAI MOTIWALLA, WENJUN LI, HUA ZHENG, PATRICIA D. FRANKLIN “Preserving Patient Privacy When Sharing Same-Disease Data”, source:” <https://dl.acm.org/doi/pdf/10.1145/2956554>”, [accessed: 13 october 2016]

Jordan P. Richardson, Cambray Smith, Susan Curtis, Sara Watson, Xuan Zhu, Barbara Barry , Richard R. Sharp, “Patient apprehensions about the use of artificial intelligence in healthcare”, source: <https://www.nature.com/articles/s41746-021-00509-1>, [ accessed: 21 September 2021]

Scheibner J , Raisaro JL , Troncoso-Pastoriza JR , Ienca M , Fellay J , Vayena E , Hubaux J, “Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis “, source: “[10.2196/25120](https://doi.org/10.2196/25120)”, [accessed: 25-02-2021]

Riley Taitingfong, Cinnamon S Bloss, Cynthia Triplett, Julie Cakici, Nanibaa’ Garrison, Shelley Cole, Julie A Stoner, Lucila Ohno-Machado , “A systematic literature review of Native American and Pacific Islanders’ perspectives on health data privacy in the United States “, source: <https://doi.org/10.1093/jamia/ocaa235>, [accessed:  15 October 2020]

Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert, Rickmer F. Braren, “Secure, privacy-preserving and federated machine learning in medical imaging”Source: <https://www.nature.com/articles/s42256-020-0186-1> , [accessed: 8th June 2020]

(IBM, “Cost of data breach 2022”, source: <https://www.ibm.com/reports/data-breach> , 2022)