



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: H
INFORMATION & TECHNOLOGY

Volume 21 Issue 1 Version 1.0 Year 2021

Type: Double Blind Peer Reviewed International Research Journal

Publisher: Global Journals

Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Artificial Intelligence in Health Policy – A Global Perspective

By Immanuel Azaad Moonesar & Ruchi Dass

Abstract- Introduction: Artificial Intelligence has become the new frontier for digital transformation. For healthcare, AI brings a paradigm shift, powered by increasing healthcare data availability and the rapid progress of analytics techniques globally.

Objective: Several hypotheses are set forward to design a policy framework for AI technologies was discussed. This review also suggests a framework that we reflect is a better case involving "responsible AI" and "permission less innovation."

Methodology: In this perspective review, AI insights into countries such as the USA, UAE, UK, and the European Union using secondary research.

Results: Policy recommendations would impact multiple stakeholders in the value chain. The efficient and responsible use of AI tools would mean culture, data management, technology shifts in the industry, and required up-grading and training professionals for better coordination

Keywords: artificial intelligence, privacy laws, future of AI, health policy, responsible AI.

GJCST-H Classification: 1.2



Strictly as per the compliance and regulations of:



Artificial Intelligence in Health Policy – A Global Perspective

Immanuel Azaad Moonesar^α & Ruchi Dass^σ

Abstract- Introduction: Artificial Intelligence has become the new frontier for digital transformation. For healthcare, AI brings a paradigm shift, powered by increasing healthcare data availability and the rapid progress of analytics techniques globally.

Objective: Several hypotheses are set forward to design a policy framework for AI technologies was discussed. This review also suggests a framework that we reflect is a better case involving "responsible AI" and "permission less innovation."

Methodology: In this perspective review, AI insights into countries such as the USA, UAE, UK, and the European Union using secondary research.

Results: Policy recommendations would impact multiple stakeholders in the value chain. The efficient and responsible use of AI tools would mean culture, data management, technology shifts in the industry, and required up-grading and training professionals for better coordination. To achieve the promise AI technology brings in and its efficient use, these policy suggestions will form the policy framework upon which key stakeholders collaborate. The key factors and elements crucial for informing policy with sufficient evidence include collaboration, facilitation, oversight management, quality structure, education, benchmarking and best practices, ethics and accountability and 'responsible AI.'

Conclusion: The review can influence policymakers and stakeholders to develop AI and data privacy policies and guidelines across countries globally in healthcare facilities, especially during the current drive towards the future of AI. Future research could investigate the effect of specific variables on healthcare facility users' perceptions that might influence AI use and data privacy.

Keywords: artificial intelligence, privacy laws, future of AI, health policy, responsible AI.

I. INTRODUCTION

In the contemporary era, many governments worldwide shifted its' policy research agenda to understand and assess the uses of social media, e-services, digital transformation, smart cities, open government data, robotics, deep learning, big data, machine learning blockchain, and artificial intelligence. The idiom "artificial intelligence" was first coined by John McCarthy at a famously held workshop at Dartmouth

College, Hanover, USA, during 1956. According to John McCarthy, the father of Artificial Intelligence (AI) defined as "the science and engineering of making intelligent machines," and researchers define AI as the aim to "mimic human cognitive functions." For healthcare, AI is bringing a paradigm shift, powered by increasing healthcare data availability and the rapid progress of analytics techniques. AI generally encompasses of various activities such as machine learning, robotics, and deep learning. For the context of this perspective review, deep learning is where there are artificial neural networks. Secondly, machine learning is making machines that learn from data, such as Automatic Teller Machine cheque readers. And finally, robotics is creating devices and machines that move, such as autonomous vehicles.

AI has become the new edge for digital transformation. Many factors support and drive the fast and powerful evolution of Artificial Intelligence across industries. Most common amongst these are:

Access to sophisticated, fast, and cost-effective computing (processing) tools, hardware, and software and applications,

Availability of large (big) and longitudinal data sets generated by digital efforts worldwide and technologies like IoT.

Availability of open-source coding resources, online communities, users (coders and managers) sharing know-how.

However, many companies are still struggling with real business value, and many Governments are still toying with the idea. In a nutshell, everyone wishes to weigh the risk and reward before committing to such an expensive effort. The AI business risks can around [1, 17, 18]:

- Lack of transparency,
- Bias and discrimination/ social inequality,
- Accountability,
- Privacy and security of data and processes,
- Audit trails,
- Process oversight,
- Legal and regulatory governance, and
- Outcomes leading to mental or physical harm.

Hence, with the growing market potential and interest in AI, it is imperative to develop a thought-through regulatory and legal framework on the adoption

Author α: Associate Professor- Health Administration and Policy, Mohammed Bin Rashid School of Government.

e-mail: immanuel.moonesar@mbrsg.ac.ae

Author σ: Non-resident Fellow, Mohammed Bin Rashid School of Government. e-mail: druchibhatt@gmail.com

and use of AI. Several hypotheses are set forward to design a policy framework for AI technologies; the authors will discuss them. This review also suggests a framework that we think is a better case involving "responsible AI" and "permission less innovation."

Size of the problem

As per the Grand View Research report, The global artificial intelligence market size was valued at USD 62.3 billion in 2020 and is expected to grow at a compound annual growth rate (CAGR) of 42.2% from 2020 to 2027. [1] AI decision-making applications that use algorithmic, neural networks, deep learning, expert and learning systems are used in education, digital imaging, healthcare, manufacturing, robotics, government, supply chain, manufacturing, and production can replace humans for a variety of processes and tasks. This dependency on automated AI-centric systems has raised enormous concern about over-allocating resources towards mitigating AI's most extreme impacts.

II. UNDERLYING FACTORS

Regulations: There is an ongoing global debate on opaque AI systems, data protection regulations, and the lack of transparency on automated data processing. Regulatory approvals and interventions must have access and understanding of concrete definitions; however, the consensus around AI has been broadly worded, an elusive feat, especially in policy discussions. The United Kingdom and the European Union have already implemented AI policies that promote trustworthy AI. Europe has some stringent digital rules that are more strict than HIPAA rules in the US. For example, Article 22 stipulates that citizens cannot be submitted to medical decisions generated by an automated source. [2]NIST's revised data standards have become central to AI policy under the US's Trump order. [3]

Policy versus Practice: AI advocates and researchers define AI that highlights its usability, functionality, and process. On the other hand, while designing Policy frameworks, policymakers recognize AI as a tool that should have caution, sensitivity, and prudence like human beings compared to human behavior. Hence, sometimes policies tend to over accentuate concern on the future use of these technologies, ignoring current usability and present-day issues. [4]

Human Rights: Advances in technology suggest that industries shall be moving on to a high-level machine intelligence and super-intelligent AI in a few decades. Many recommend it as not safe for humanity. AI may take up a lot of human jobs and work. Although there may be some ambiguity and uncertainty around how jobs and human effort will transition to AI, governments are brainstorming on AI strategy to better prepare systems, users, and processes to minimize negative

impact. There is consideration required to understand the destructive power of AI as well. As suggested by Taddeo & Floridi (2018), there is a pertinent risk that the AI arms race [5] can trigger inadvertent development and AI use. Hence, in addition to Fairness, Accountability, Transparency, and Ethics, human rights serve as a complementary framework for guiding and governing AI and machine learning research and development. [6]

Governance: Here, we are taking the example of healthcare as an industry to understand governance-related challenges. Healthcare, as an industry, has established processes and frameworks. The fast pace development and roll-out of AI-related projects may hamper such frameworks. Hence, to maintain such processes and frameworks, an overarching framework must assess and establish potential areas of impact and how regulations may view these changes. Innovation in processes, analysis, and research needs to be developed in the light of maintaining transparency, accountability, and social impact/public interest, as stated in the problem statement above. In addition to these frameworks, it is also essential to develop skill sets amongst the subject matter experts and the user community to plan, assess, and evaluate the best use case of AI for their respective industries.

III. POLICY RECOMMENDATIONS & IMPLICATIONS



Fig. 1: Recommendations on the AI policy framework

Policy suggestions below would impact multiple stakeholders in the value chain. This is because efficient and responsible use of Artificial intelligence tools would mean culture, data management, technology shifts in the industry, and required up-grading and training professionals for better coordination. To achieve the promise AI technology brings in and its efficient use, these policy suggestions will form the policy framework upon which key stakeholders collaborate. The key factors and elements crucial for informing policy with sufficient evidence include collaboration, facilitation, oversight management, quality structure, education, benchmarking and best practices, ethics and accountability and 'responsible AI.'

Given the risk imposed with the advancement and uptake of AI amongst industries, here are seven high-level recommendations summed up in Figure 1:

Collaboration: AI development and implementation should involve multi-stakeholders to collaborate for social, economic, ethical, and legal implications of AI. Public funding should be provided wherever possible to drive mandates for such collaborations nationally and internationally. Collaborations and partnerships should promote knowledge sharing, building access to information, and innovation. Hence, policymakers need to collaborate with AI experts and researchers to design and implement frameworks that facilitate research initiatives and are aligned with the technical practice of AI gapping the divide between policy and practice.

Facilitation: Involvement of experts and relevant stakeholders in discussing challenges and possible safeguards against threats. Both Public and Private sectors should pool inappropriate funding for the R&D

efforts pertaining to AI. All parties (regulatory and industry stakeholders) should come together to provide access to resources that help facilitate digitization, building data access, and encouraging incentives like tax credits for both profit and non-profit research that prioritizes transparency and evidence-based validation. Policy frameworks should enable data access by creating a cooperation culture among policymakers, experts, technology users, and the general public.

Oversight management: Safety and efficacy of AI are contingent upon well-thought-out risk management approaches and processes to align standards and drive compliance. "What the eye doesn't see, and the mind doesn't know, doesn't exist" [7]. Hence, awareness of possible misuse, abuse, and bias is necessary amongst both researchers and policymakers alike to influence norms, design, and applications, proactively analyzing and flagging potential misuse. The policy framework should highlight all actors- roles, process risks, liabilities, and incentives to highlight opacity, bias, discrimination, inefficiency, and any other negative impact (responsible disclosure).

Quality structure: It is vital that stakeholders understand AI risk distribution and liability while using AI tools. An ideal AI structure/ technological framework should support:

Guiding principles of being explainable, transparent (auditable), and fair (unbiased)

And augment human capabilities and maintain human well-being by being safe, ethical, and equitable (human-centric).

Hence quality assurance should be taken into perspective while designing, developing, and deploying AI tools. Policy frameworks also need to match real-world workflows, usability principles, and end-user needs. These AI-driven systems should also solve the redundant, disjointed, and dysfunctions of the technology/ operational systems.

Education: In addition to understanding the risk and opportunities of AI, it is also important to realize that an uneven distribution of technology and resources can hamper equitable access to AI resources. Hence, policymakers should influence investments in building AI infrastructure, training personnel, and building an engaging community of users and researchers that help demonstrate AI value leading to voluntary adoption and standards compliance. The education interventions with stakeholder involvement should also encourage keeping these frameworks up-to-date and perceptive to upcoming challenges.

Benchmarking and Best Practices: Microsoft, Accenture, and other global companies are members of the Partnership on AI, dedicated to research, discussion, and best practices publication. And the Future of Life Institute has published perhaps the most

comprehensive set of principles called the Asilomar AI Principles, signed by thousands of scientists and others, including Stephen Hawking, Elon Musk, and Dennis Hassabis.

Ethics and Accountability: AI adoption will only progress and reach its potential if it is used ethically to protect its users (that is, humans). A digital economic policy has been adopted by almost 40 countries, including the US and the European Union. For private organizations, the personal data protection commission (PDPC), Singapore, proposed a model that guides how ethical principles can be converted into implementable practices as per the World Economic Forum regulations. In 2018, the UK also mandated five principles that could become the basis for a shared ethical AI framework. These include [8]:

Development for common good

Act with fairness and clarity

Preserve data rights and privacy of communities.

AI to help improve citizens' cognitive intelligence alongside artificial intelligence.

Should not be used to destroy or deceive human beings autonomously.

IV. RESPONSIBLE AI

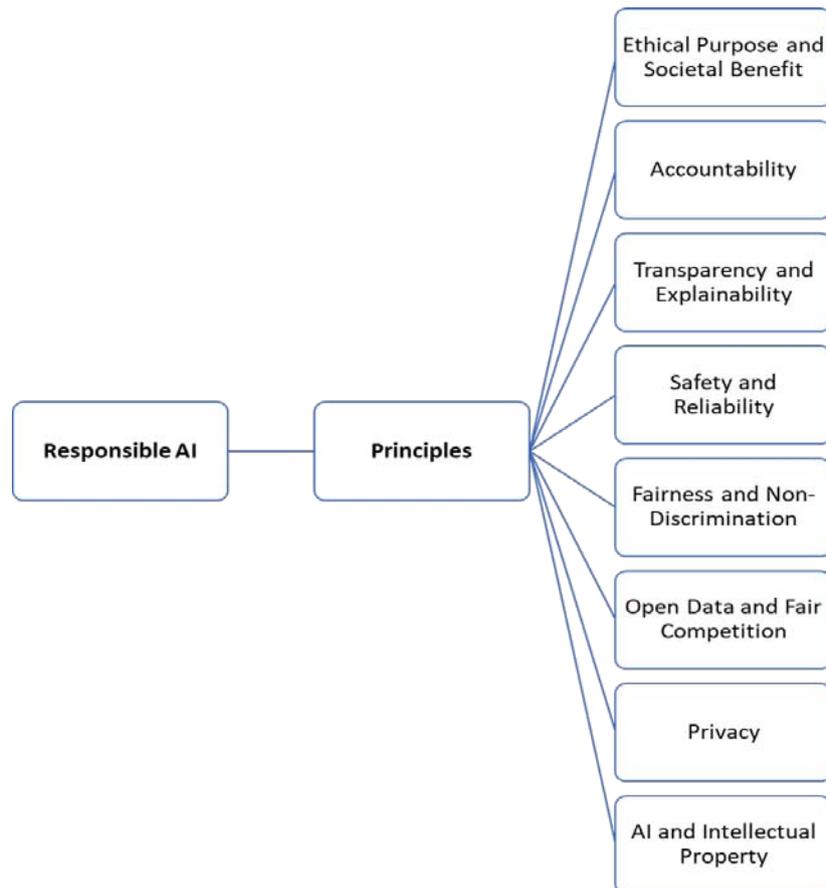


Fig. 2: Responsible AI overarching Principles

Responsible AI is a framework that emphasizes ethical, accountable, and transparent use of AI technologies congruous with human rights, societal norms, user expectations, and organizational values. The overarching eight principles of AI ethics and reliability as adapted from the Responsible AI framework by IT tech law is mentioned in Figure 2. [9]

Independent non-profit bodies like AI-Global [10] are an open platform combining reports, standards, government policies, models, open/available datasets, and open-source software to support affiliates better circumnavigate the AI landscape and directly align and link with the experts who are creating these valuable resources. For instance, the Institute for Ethical AI & Machine Learning is a UK-based research center that conducts highly-technical research into processes and frameworks that support the responsible development, implementation, deployment, and operation of machine learning systems.[11] Many other Data & AI Authorities also emphasize prioritizing ethics in AI and providing practical tools for responsible AI. Others like Certifai [12] work as an AI Risk Scanner application that detects and scores vulnerabilities in any black-box AI model. These application/tools primarily answer the questions around: Explainability- what was predicted and how "x" was predicted?

Fairness- Is it ethical or unfair to a particular group?

Robustness- Can the model be fooled? How robust is the model?

Compliance- Does the design comply with industry regulations?

Governments, private businesses, and non-governmental organizations across the Middle East region are recognizing the shift globally towards AI and advanced technologies. PWC [13] estimates that the Middle East is expected to ensue 2% of the total global benefits of AI in 2030, which is equal to US\$320 billion.

The UAE's national program on Artificial Intelligence aims at enhancing Government performance and efficiency. Recently, the Government of Dubai, Smart Dubai, published Dubai's Ethical AI Toolkit. The toolkit has been created to provide hands-on support across a metropolitan ecosystem. It supports academia, industry, and citizens in understanding how AI systems can be utilized responsibly. It comprises principles and guidelines and a self-assessment tool for developers to assess their platforms. [14] Europe's Communication on Artificial Intelligence, 2018 [15], submitted a report on the implication of AI implementation from the angle of safety and liability. As two-thirds of the value creation by AI contributes to the B2B segment, it is a call for us all researchers, academicians, business owners, governments, and industry leaders to come together and provide due consideration to ethical automation with the use of such technologies.

Table 1: Potential Solutions to AI drawbacks and implementation considerations

Drawbacks	Ethical challenge	Implementation considerations
1 AI Black box	Unexplained Predictions	Build Transparency
Though AI algorithms can learn from massive amounts of data and internalize them to make decisions, these algorithms could be a black box to even their creators. [16]	Predictions and decisions without reasons	<ul style="list-style-type: none"> a) Transparent design, Interpretable output- Develop decision or prediction model with its explanation. b) Model Inspection-> Model explanation->Outcome explanation c) Use what can be explained. Treat self-learning neural networks and solutions with care.
2 Algorithmic Complexity	Difficult to understand and comprehend the "how?"	Provide adequate training & Validate models
There is more emphasis on models to give smart decisions than ethical ones. Technical secrecy and complexity can be deception	Little understanding or skills around comprehending the algorithm, its functional elements, modus operandi, and relationship across system may blind decision making	Training is required for the end professional to interpret and explicably understand the AI models and the application. Enough test cases (vertical domain) should be run to validate the results of AI.

3 Data quality challenges	Biased data, Biased results	Data collection and processing need to be audited
If data collection is flawed, and the algorithm is narrow or subjective- it can provide biased results that emphasize a stereotype or not take the breadth of factors into account.	Data sets need to be sufficiently large and broad. The smaller size of the data sets can lead to inaccurate or biased results.	High-quality data are essential to train and run an Artificial Intelligence system. These need to be audited so that we can be prevented or detect, report, and neutralize at the earliest.[17]
4 Data Privacy & Cybersecurity	Vulnerabilities introduced in systems can expose private data	a) Accountability, disclosure, and compliance to prevent data theft is the need of the hour b) Robust systems that can withstand adversarial attacks
While introducing AI into systems, vulnerabilities can creep in, leading to data theft.	Cyber intrusion risks Privacy risks Adversarial attacks	Stronger disclosure laws requiring firms to comply to data privacy (data minimization; reporting security and privacy breaches) data protection impact assessments (DPIAs) should be performed before utilizing any personal data. Neural fuzzing can be used to test large amounts of random input data within the software to identify its vulnerabilities. [18] Compliance to data privacy regulations (European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

V. CONCLUSION

The review can influence policymakers and stakeholders to develop AI and data privacy policies and guidelines across countries globally in healthcare facilities, especially during the current drive towards the future of AI. Future research could investigate the effect of specific variables on healthcare facility users' perceptions that might influence AI use and data privacy.

VI. STATEMENTS

Acknowledgment: I would like to acknowledge the support from the Dubai Health Authority and the Mohammed Bin Rashid School of Government, Dubai, United Arab Emirates. We would also like to acknowledge the Alliance for Health Policy and Systems Research at the World Health Organization for financial support as part of the Knowledge to Policy (K2P) Center Mentorship Program [BIRD Project].

Statement of Ethics: Not applicable

Disclosure Statement: The authors have no conflicts of interest to declare.

REFERENCES RÉFÉRENCES REFERENCIAS

1. Artificial Intelligence Market Size, Trends Analysis Report By Solution (Hardware, Software, Services), By Technology (Deep Learning, Machine Learning), By End Use, By Region, And Segment Forecasts, 2020 - 2027 (Rep. No. GVR-1-68038-955-5). (2020). Retrieved 2020, from <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market>
2. Gourraud, P. (2020). Differences between Europe and the United States on AI/Digital Policy: Comment Response to Roundtable Discussion on AI. *Gender and the Genome*, 4, 247028972090710. doi:10.1177/2470289720907103
3. Weber, R. (2019). Lawyers say NIST's revised data standards should be central to AI policy under trump order. *Inside Cybersecurity*, Retrieved from <https://search-proquest-com.lbs.idm.oclc.org/docview/2242766558?accountid=16482>
4. Krafft, P. M., Young, M., Katell, M., Huang, K., & Bugingo, G. (2020). Defining AI in Policy versus Practice. *Proceedings of the AAAI/ACM*

- Conference on AI, Ethics, and Society. doi:10.1145/3375627.3375835
5. Taddeo, Mariarosaria & Floridi, Luciano. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*. 556. 296-298. 10.1038/d41586-018-04602-6.
 6. Corinne Cath, Mark Latonero, Vidushi Marda, and Roya Pakzad. 2020. Leap of FATE: human rights as a complementary framework for AI policy and practice. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT*20)*. Association for Computing Machinery, New York, NY, USA, 702. DOI: <https://doi.org/10.1145/3351095.3375665>
 7. "What the eye doesn't see and the mind doesn't know, doesn't exist."— D. H. Lawrence
 8. AI in the UK: Ready, willing and able? (Rep. No. HL Paper 100). (2019). Retrieved 2020, from Authority of the House of Lords website: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>
 9. Responsible AI Policy Framework (Tech.). (n.d.). Retrieved August 17, 2020, from ITechLaw.org website: https://www.itechlaw.org/sites/default/files/ResponsibleAI_PolicyFramework.pdf
 10. Digital economy is next priority: The digital readiness of government ensures business continuity, regardless of the circumstances. (2020). Retrieved from <https://ai-global.org>
 11. The Institute for Ethical AI & Machine Learning. (2020). Retrieved from: <https://ethical.institute>
 12. Cortex Certifai: Evaluate AI models for robustness, fairness, and explainability. (2020). Retrieved from: <https://cognitivescale.github.io/cortex-certifai/>
 13. The potential impact of AI in the Middle East, by PWC. (2020). Retrieved from: <https://www.pwc.com/m1/en/publications/potential-impact-artificial-intelligence-middle-east.html>
 14. https://www.smartdubai.ae/pdfviewer/web/viewer.html?file=https://www.smartdubai.ae/docs/default-source/ai-principles-resources/ai-ethics.pdf?Sfvrsn=d4184f8d_6
 15. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>. The accompanying Staff Working Document (2018) 137 (<https://eur-lex.europa.eu/legalcontent/en/ALL/?uri=CELEX%3A52018SC0137>) provided a first mapping of liability challenges that occur in the context of emerging digital technologies.
 16. Davide Castelvecchi, Can We Open the Black Box of AI?, *NATURE* (Oct. 5, 2016) (characterizing "opening up the black box" as the "equivalent of neuroscience to understand the networks inside" the brain).
 17. FRA (2018a); Barocas, S. and Selbst, A. D. (2016). Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf
 18. AlMarzooqi, F. M., Moonesar, I. A., & AlQutob, R. (2020). Healthcare Professional and User Perceptions of e Health Data and Record Privacy in Dubai. *Information*, 11(9), 415. <https://doi.org/10.3390/info11090415>.