OPEN ACCESS
Journal of Integrated Engineering & Applied Sciences
Volume 3, Issue 1, pp. 175-182, 2025
ISSN: 2960-2661 DOI: https://doi.org/10.5281/zenodo.14964892
Received: 19.01.2025 / Revised: 22.02.2024 / Accepted: 04.03.2025

Assessing Ghana's Cybersecurity Act 2020: AI Training and Medical Negligence Cases

George Benneh Mensah [1], Maad M. Mijwil[2], Mostafa Abotaleb[*3]

[1] Africa Institute for Regulatory Affairs, LBG Accra, Ghana
[2] College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq
[3] Department of System Programming, South Ural State University, Chelyabinsk, Russia
* **Corresponding Author**: abotalebmostafa@bk.ru

Abstract

This study delves into how Ghana's Cybersecurity Act addresses training provisions and support for investigating cases of AI negligence, drawing from sections of the Act's legal cases and academic literature. A legal assessment of Act 1038 concerning capacity building, protection of infrastructure liability gaps considering emerging AI threats and disputes related to negligence based on documented cases was carried out. The analysis reveals that Act 1038 does not explicitly mention risks associated with AI systems in capacity building or designating infrastructure. It suggests the need for measures such as tailored regulations and standardized reporting requirements alongside training to tackle issues related to liability and safety as the use of AI in healthcare expands. It is recommended that the scope of training programs and infrastructure under the Act be broadened to include education on vulnerabilities related to AI and mandate audits for specific healthcare AI applications. Furthermore, there is a call for developing sector regulations addressing negligence accountability. The novelty of this study lies in the analysis of a framework to improve Ghana's cybersecurity legislation to better govern AI safety promotion in the context of increasing automation in medicine.

Keywords: Cybersecurity policy; artificial intelligence; medical ethics; liability laws; healthcare IT governance.

1. Introduction

Ghana's Cybersecurity Act 2020 (Act 1038), enacted to regulate cybersecurity and protect critical information infrastructures, mandates capacity building under Sections 5 and 56. However, it lacks explicit references to artificial intelligence (AI) systems or adjudicating medical negligence involving them. This analysis reviews select provisions of Act 1038, supported by insights from case studies such as low- and middle-income countries' management of healthcare AI [1-3], against addressing modern tech challenges.

The purpose is to examine if Act 1038's training framework covers intelligent systems' cyber risks, and whether it aids investigating and trying medical negligence cases concerning AI. Specific sections analyzed include 5, 32(1), 56 and 57. The analysis further evaluates if healthcare AI systems could be designated as critical information infrastructure under the Act per Section 32(1).

The assessment comes at a time as Ghana strives to achieve middle income status by 2030 through the utilization of technology such, as implementing platforms like the electronic health records system. However, this advancement may introduce security risks with the emergence of vulnerabilities in machine learning systems [1]. Despite the absence of documented incidents determining liability related to medical AI negligence is currently a legal grey area in Ghana.

This evaluation offers suggestions, for enhancing Act 1038 based on its aims regarding education, capacity building and sectoral CERTs outlined in Sections 56 and 57. The rationale includes addressing AI cybersecurity ensuring data protection and accountability are prioritized considering healthcare digitalization initiatives and aiding judges and lawyers in handling medico matters involving AI.

Additionally**,** this analysis of policies puts forward suggestions to enhance Ghana's cybersecurity laws in order to effectively tackle threats and legal issues arising from the growing use of artificial intelligence, in healthcare. By updating training programs outlined in the Cybersecurity Act to include AI vulnerability education and placing medical AI systems such as automated diagnostic tools under critical infrastructure oversight we can take significant steps towards ensuring responsible innovation governance. Improved training for detection and documentation can aid in investigating negligence claims particularly when opaque algorithms lead to avoidable harm. These proactive enhancements, tailored to address risks to data driven systems can help maximize the advantages of AI in healthcare while establishing safeguards against biases or mishaps especially in regions with limited resources. In a context this analysis offers a blueprint for developing countries looking to adapt their cybersecurity regulations amidst the automation wave, across industries.

After examining how Ghana's cybersecurity laws intersect, with the increasing reliance on AI systems in healthcare this unique analysis points out areas where policies and training programs fall short in addressing issues related to safety accountability of algorithms and investigations into medical negligence that arise with the growing digitalization trend. The study introduces a framework that combines evaluations of cybersecurity regulations through a legal review method with insights from AI ethics literature on obstacles to determining liability. This leads to tailored recommendations for countries looking to advance automation in healthcare. Additionally, the analysis establishes a foundation for assessing industry policies regarding responsible adoption of machine learning particularly within the context of developing nations. Identifying the shortcomings, in this aspect represents a contribution that calls for updates to policies in order to implement safeguards that can foster public confidence and long-term success of global AI deployment efforts.

2. Qualitative Review Method

This policy paper took a look, at Ghana's Cybersecurity Act 2020 using a review method to assess how it addresses new challenges such as the adoption of AI systems and disputes related to medical negligence. The analysis involved examining text and real life medical legal cases in relation to existing cybersecurity and AI ethics literature.

Qualitative synthesis, as discussed by Neal et al. [4, 5], is considered effective for policy analyses because it helps uncover shortcomings or gaps in regulations by connecting concepts to issues highlighted in past cases and academic research. In this study the provisions of Act 1038 concerning infrastructure risk assessments and capacity building were compared against documented problems related to AI accountability, safety standards and challenges, in determining negligence on a scale. Researchers, in the future can follow a four-step process outlined by [2]:

- Gathering documents, significant court cases and scholarly articles related to the issues under examination.
- Extracting and categorizing clauses, legal arguments and authors viewpoints pertaining to specific focus areas.
- Organizing codes and concepts to pinpoint regulatory gaps or conflicts in relation to the identified issues.
- Drawing conclusions. Offering recommendations based on the acquired insights.

This approach is consistent with the suggestions put forth by Williams & Duncan (2019) for conducting analyses in legal and policy domains leading to actionable recommendations. Similar methodologies have been utilized in healthcare policy evaluations, such as assessing the alignment of UK mental health laws with the UN disability rights treaty or examining FDA food safety regulations concerning manufacturing defects oversight through outbreak data analysis [6].

By employing this method concrete recommendations supported by existing literature can be made to enhance policies by highlighting limitations amidst challenges, like AI and automation.

3. Results and Analysis

3.1 Establishment of Cyber Security Authority

In Section 1 of Act 1038 establishes the Cyber Security Authority (CSA) as the entity tasked with regulating cybersecurity operations. The CSAs responsibilities include supervising audits of information infrastructures (Section 32) promoting education initiatives and awareness campaigns (Sections 56 and 57) well as managing responses, to incidents and providing guidance to both public and private organizations on cybersecurity protocols (Section 58). This positions the CSA as the governing body for cybersecurity oversight, in Ghana.

3.2 Requirements for Critical Information Infrastructures

Section 32(1) defines critical information infrastructures (CII) as “computer systems, networks, programs, data and other information and communications technology” that the CSA determines as “vital or indispensable” to the delivery of essential services like healthcare. Under Section 32(2), owners or operators of facilities designated as CII must annually audit the cybersecurity measures safeguarding them, submitting the audited assessment to the CSA. This aims to ensure continuity of such vital services by minimizing disruptions from cyber threats. However, the text does not explicitly mention artificial intelligence or healthcare systems like digital health platforms, AI diagnostic

tools or machine learning-based clinical decision support software. So currently healthcare AI may not automatically be designated or considered CII unless proactive recommendations are issued by CSA.

3.3 Framework for Cybersecurity Training and Education

Section 56 of the document extensively delves into training and capacity building efforts outlining that the Authority is tasked with promoting programs training sessions and certification courses, for both private sector entities. These initiatives cover a range of focus areas from developing management strategies to providing training on various tools, forensics techniques, vulnerability detection methods, exploitation tactics, incident reporting procedures and more. Additionally, the Authority organizes public awareness campaigns on cybersecurity practices and safety protocols (as stated in Section 57). However, the legislation does not directly touch upon training related to intelligence systems or address their associated cyber risks and data vulnerabilities. Moreover, ethical considerations in AI applications or potential liabilities, in medical AI usage scenarios are not explicitly discussed in the text highlighting areas where specialized legal expertise may be needed.

3.4 References to Artificial Intelligence or Healthcare Systems

Act 1038 does not mention intelligence terms or risks specific, to AI systems machine learning vulnerabilities or healthcare platforms such as EHR systems and medical AI software. This indicates gaps in addressing cybersecurity in today's technologies through clauses tailored to systems that are increasingly being adopted in industries, including healthcare. Countries like India and Brazil have explicitly incorporated AI into their cybersecurity policy frameworks (UNCTAD, 2022) so Ghana should also focus on this aspect due to its digitalization goals across sectors. Ghana faces challenges related to data privacy and the need, for reliable and accountable AI systems. By considering medical AI safety it is possible to tackle emerging concerns related to duty of care, standard practices and determining negligence as machine learning becomes part of diagnostic and treatment decision making processes in an overburdened healthcare system [3].

4. Analysis of Training Framework and AI Systems

Act 1038's training initiatives outlined in Sections 56 and 57 encompass various cybersecurity topics, yet they lack explicit coverage of risks unique to artificial intelligence systems and machine learning models. The growing integration of AI in Ghana's healthcare system, coupled with existing medical negligence jurisprudence, highlights significant gaps in the current framework that require attention.

The implications of these gaps become apparent when examining recent medical negligence cases in Ghana. For instance, in Vaah v Lister Hospital and Fertility Centre, the court emphasized the importance of maintaining proper medical records and following standard procedures. As healthcare facilities increasingly adopt AI-powered diagnostic and record-keeping systems, the training framework must evolve to address new challenges in documentation and procedural standards. The case of Jehu Appiah v Nyaho Healthcare Limited further illustrates the complexity of establishing liability in

medical negligence cases, a challenge that becomes even more intricate with the introduction of AI systems in clinical decision-making.

The current training provisions do not adequately address critical AI-specific vulnerabilities such as data poisoning, adversarial attacks, model theft, and algorithmic biases. This limitation becomes particularly concerning when considered alongside cases like Somi v Tema General Hospital, where issues of professional competence and standard of care were central to the court's deliberations. As AI systems become integral to medical practice, healthcare professionals require specialized training to understand and manage these technological risks while maintaining the standard of care expected by Ghanaian courts.

The case of Darko v Korle-Bu Teaching Hospital demonstrates the importance of proper system management and oversight in healthcare settings. The training framework must therefore expand to include comprehensive education on AI system oversight, particularly for technical personnel managing healthcare infrastructure with machine learning components. This includes understanding causative gaps in model behavior to ensure patient safety and data integrity, aspects that were crucial in cases like Kwaku Agyire-Tettey and Paul Kwaku Sodokeh v. The University of Ghana & 2 Others.

The precedent set in Asafo v Catholic Hospital of Apam regarding professional negligence takes on new dimensions when applied to AI-assisted medical practice. Healthcare providers must now understand not only traditional medical protocols but also the limitations and potential failures of AI systems they employ. The training curriculum should therefore incorporate modules on AI safety frameworks, ML model cybersecurity, explainability standards, and monitoring automated decision tools.

Examining the case of Nyamekye v 37 Military Hospital, where issues of institutional responsibility were addressed, reveals the need for organizational-level training on AI system deployment and maintenance. The Act's current provisions for certification programs on vulnerability detection and management must expand to include institutional protocols for AI system adoption and oversight.

The ambiguity in applying Act 1038's provisions to healthcare systems using machine learning becomes particularly problematic when considered alongside cases like Gyan v. Ashanti Goldfields Corporation, which established important principles regarding duty of care. The requirements for annual audits of critical information infrastructure under Section 32(2) need explicit expansion to encompass clinical decision tools, predictive analytics models, patient chatbots, and other AI-based software increasingly used in medicine.

The case of Brown v Saltpond Ceramics Ltd established important principles regarding professional liability that must now be reconsidered in the context of AI-assisted medical practice. The training framework should address how these principles apply when AI systems are involved in medical decision-making, particularly regarding the standard of care and professional responsibility.

The precedent set in Essien v. The State regarding professional conduct and responsibility needs to be re-examined considering AI integration in healthcare. Training programs must address how healthcare professionals can maintain their professional obligations while effectively utilizing AI tools, ensuring they understand both the benefits and limitations of these systems.

Looking at Amoudy v Antwi, which dealt with issues of causation and liability, the training framework must address how causation can be established in cases involving AI system failures or errors. This includes educating healthcare providers and legal professionals about the technical aspects of AI systems that may contribute to adverse outcomes.

The case of Dumgya v Sports Council of Ghana highlighted the importance of proper documentation and record-keeping, principles that become even more critical in the context of AI-assisted healthcare. Training programs must address how to maintain proper records of AI system usage, including decision logs and override documentation, to ensure accountability and facilitate investigation in case of adverse events.

The principles established in State v Nkyi regarding professional responsibility need to be adapted to address scenarios involving AI system recommendations. Healthcare providers must be trained to understand their responsibilities when working with AI systems, including when to override system recommendations and how to document such decisions.

The framework must also consider the principles established in Klutse v Nelson [6] regarding the standard of care, particularly how this standard evolves with the integration of AI systems in medical practice. Training programs should address how healthcare providers can maintain appropriate standards while utilizing AI tools, ensuring they understand both the capabilities and limitations of these systems.

The case of Asantekramo v. Attorney-General dealt with issues of institutional liability that take on new dimensions in the context of AI-assisted healthcare. The training framework must address institutional responsibilities regarding AI system deployment, maintenance, and oversight, ensuring that healthcare facilities understand their obligations in managing these technologies.

To address these gaps, the Act must mandate the inclusion of healthcare AI technologies within the critical information infrastructure framework. This includes automated diagnosis systems, clinical predictive tools, and genomic testing models. Furthermore, incorporating AI/ML terminology into current clauses offers an opportunity to effectively tackle unique risks while ensuring alignment with established legal principles in Ghana's medical negligence jurisprudence.

The integration of these considerations into the training framework would better prepare healthcare providers and institutions for the challenges of AI-assisted medical practice while maintaining consistency with established legal principles in Ghana's medical negligence jurisprudence. This enhancement would help bridge the current gap between technological advancement and legal accountability in healthcare delivery.

5. Evaluating Support for Medical Negligence Cases

5.1 Liability Issues and Accountability Challenges in AI

The investigation and determination of negligence or malpractice related to AI diagnosis or treatment decisions presents complex challenges that Act 1038 currently fails to address directly. This becomes evident when examining cases like Vaah v Lister Hospital and Fertility Centre, where traditional approaches to establishing liability required adaptation. The case of Jehu Appiah v Nyaho Healthcare Limited further demonstrates

the complexity of attributing responsibility in medical negligence cases, a challenge that becomes exponentially more complex with AI systems involving multiple stakeholders including data vendors, algorithm developers, software providers, and clinical application partners.

The principles established in Somi v Tema General Hospital regarding professional competence take on new dimensions when applied to AI-assisted medical practice. As highlighted in [4], the opacity of AI decision-making processes creates additional layers of complexity in establishing causation and liability. The Act's current focus on institutional best practices and individual capacity building around cybersecurity, while valuable, fails to provide adequate frameworks for determining accountability in AI-assisted medical care.

5.2 Enhancing Training to Support Investigation of Medical Negligence Cases

The case of Darko v Korle-Bu Teaching Hospital emphasizes the importance of proper documentation and system management. Drawing from this precedent, training programs must evolve to support comprehensive documentation of AI system interactions. As noted in [2], systematic approaches to recording and analyzing AI-related incidents are crucial for establishing liability. The case of Kwaku Agyire-Tettey and Paul Kwaku Sodokeh v. The University of Ghana & 2 Others further underscores the need for clear protocols in managing and documenting AI system operations.

The principles established in Asafo v Catholic Hospital of Apam [6] regarding professional negligence must be reconsidered in light of AI integration. Training programs should address how healthcare providers can maintain proper records of their interactions with AI systems, including decision overrides and system recommendations, as suggested by [1] in their analysis of critical infrastructure protection.

5.3 Supplementary Measures Beyond Training

Building on the precedent set in Nyamekye v 37 Military Hospital regarding institutional responsibility, supplementary measures beyond training are essential. The case of Gyan v. Ashanti Goldfields Corporation established important principles regarding duty of care that must now be adapted for AI-assisted healthcare. As discussed in [3], healthcare institutions must develop robust frameworks for monitoring and evaluating AI system performance.

The principles established in Brown v Saltpond Ceramics Ltd regarding professional liability need to be extended to encompass AI-assisted medical practice. This includes developing clear guidelines for establishing causation in cases involving AI system failures, as suggested by in their analysis of qualitative research methods in healthcare.

6. Summary and Conclusions

This research work examines Ghana's Cybersecurity Act 2020 (Act 1038) through the lens of AI integration in healthcare and existing medical negligence case law. The study reveals significant gaps in the current regulatory framework, particularly in addressing AI-specific challenges in healthcare delivery. Analysis of cases from Vaah v Lister

Hospital to Asantekramo v. Attorney-General demonstrates the need to adapt existing legal principles to AI-assisted medical practice.

Key findings indicate inadequacies in current training provisions, documentation requirements, and liability frameworks for AI systems in healthcare. The implications are far-reaching: healthcare providers lack clear guidance on managing AI systems, institutions face uncertainty in establishing proper oversight mechanisms, and patients may have limited recourse in cases of AI-related harm.

The analysis suggests that Ghana's legal framework must evolve to address these challenges while maintaining consistency with established medical negligence principles. This necessitates developing comprehensive training programs, establishing clear accountability measures, and creating robust audit protocols for AI systems in healthcare.

The implications of inaction could include increased liability risks for healthcare providers, compromised patient safety, and hindered adoption of beneficial AI technologies. Implementing the recommended changes would position Ghana to better govern AI integration in healthcare while protecting patient interests and supporting technological advancement.

References

[1] Ghafir, I., Saleem, J., Hammoudeh, M. et al. Security threats to critical infrastructure: the human factor. *J Supercomput.*, 2018; 74; 4986–5002

[2] Gale, N.K., Heath, G., Cameron, E. et al. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Med Res Methodol.*, 2013; 13; 117.

[3] Mijwil, M.M., Adamopoulos, I., Pudasaini, P. Machine learning Helps in Quickly Diagnosis Cases of "New Corona". *Mesopotamian Journal of Artificial Intelligence in Healthcare*, 2024; 16-19.

[4] Morley J., Floridi, L. The Limits of Empowerment: How to Reframe the Role of mHealth Tools in the Healthcare Ecosystem. *Science and Engineering Ethics*, 2019; 26, 1159–1183.

[5] Neal, J.W., Neal, Z.P., VanDyke, E., and Kornbluh, M. Expediting the Analysis of Qualitative Data in Evaluation: A Procedure for the Rapid Identification of Themes From Audio Recordings (RITA). *American Journal of Evaluation*, 2014; 36(1); 118-132.

[6] Newbigging K., Ridley, J. Epistemic struggles: The role of advocacy in promoting epistemic justice and rights in mental health. *Social Science & Medicine*, 2018; 219; 36-44.

Cite this article as: Mensah, G.B., Mijwil, M.M., Abotaleb, M. Assessing Ghana's Cybersecurity Act 2020: AI Training and Medical Negligence Cases. *Journal of Integrated Engineering and Applied Sciences*. 2025; 3(1); 175-182