Global Insights in Artificial Intelligence and Computing

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

Integrating Quality Assurance and Cyber Defense in Generative AI Applications for Healthcare Systems

Murad Khan[1*], Ahmad Bacha[2]

[1]American National University, Salem, Virginia

[2]Washington University of Science and Technology, Virginia, United States of America

[1]khanm@students.an.edu, [2]abacha.student@wust.edu

open access

Corresponding Author

Murad Khan
khanm@students.an.edu

Article History:

Submitted: 03-07-2025

Accepted: 11-08-2025

Published: 16-08-2025

Keywords:
Generative Artificial Intelligence, Quality Assurance, Cyber Defense, Healthcare Systems, Patient Safety, Regulatory Frameworks.

ABSTRACT

Generative Artificial Intelligence (AI) is transforming the medical sphere, making it possible to achieve high-quality diagnostics, individual treatment, and informed choices. But its increased usage is causing a serious issue of data integrity, system reliability, and cybersecurity. The paper reviews how Quality Assurance (QA) and the Cyber Defense models can be combined to make healthcare systems using generative AI to be safe, accurate, and trustworthy. It looks at major methodologies, issues and new solutions that reconcile AI innovation to ethical, regulatory and security norms. Through the integration of QA validation and military-grade cyber defense, healthcare organizations will be able to have resilient, transparent, and secure AI applications that will eventually result in patient trust and improvement of overall quality of digital healthcare delivery.

Introduction

The introduction of Generative Artificial Intelligence (AI) into the healthcare industry is a shift in a new era of medical technology, which allows the newly unmatched possibilities in the diagnostics,

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

treatment planning, drug discovery, and administrative effectiveness. Nevertheless, with the growing use of AI-based systems by healthcare organizations, the necessity to maintain quality assurance (QA) and cyber defense has become a pressing one [1]. The healthcare information is one of the most sensitive types of information and generative AI models, which, in their training, use large amounts of data, raise complicated concerns about data integrity, data security, privacy, and ethical standards. This is a review of the ways quality assurance and cyber defense can be effectively combined to create safe, reliable, and trustful uses of generative AI in healthcare settings [2].

Generative AI models, such as large language models (LLMs), generative adversarial networks (GANs) or diffusion models are starting to be applied as generative medical image synthesis models, disease progression predictions, and clinical note generation tasks. Such models are more efficient and accurate, although their implementation in a clinical practice requires strict QA mechanisms that would ensure that their work is valid and they do not introduce possible mistakes that might damage a patient [3]. QA guarantees that AI systems perform as per their specifications, generate clinically meaningful results and that they are regulated in accordance to standards. In the healthcare context, we have the constant testing, verification with ground-truth datasets, biases identification, and performance measures on a variety of patient populations [4].

At the same time, digital transformation of healthcare creates a larger scope of cybersecurity threats. Certain attacks to generative AI systems include data poisoning, model inversion, adversarial manipulation, and unauthorized access to their data. Besides putting the integrity of models at risk, these threats threaten patient safety and breach compliance regulations such as the HIPAA and GDPR [5]. Thus, it is critical to consider the process of introducing powerful cyber defense measures, including encryption, intrusion detection, and secure model lifecycle management, into the AI pipeline. Cyber defense is not a process aimed at safeguarding networks or servers anymore; it should also be applied to the safeguarding of AI algorithms, datasets, and outputs [6].

QA coupled with cyber defense integration offers a holistic way of constructing resilient AI-driven healthcare systems. Quality assurance is a measure of reliability and accuracy, cyber defense is a measure of confidentiality and integrity. They collectively create a single framework that creates confidence, transparency, and obedience in the use of generative AI. This integration also enables explainability, accountability and constant improvement, which are important in the adoption of clinical and approval of regulations [7].

To conclude, the introduction provides the background of this review as it emphasizes the twofold need of QA and cybersecurity in generative AI in healthcare. It highlights the fact that medical AI faces both a bright future and a dark one, as one of its key aspects is not only innovation, but also the

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

possibility of safety, trust, and resistance to changing digital threats. These sections further discuss the mechanisms, frameworks and methodologies needed to achieve this integration successfully [8].

General Healthcare Systems Generative AI Overview

Generative Artificial Intelligence (AI) is a groundbreaking development in the field of healthcare, which provides an opportunity to produce, model, and forecast sophisticated medical information with astounding accuracy. Notably, in contrast to conventional AI models, which classify or analyze existing data, generative models are able to generate real, new data (medical imaging, patient records, and molecular geometry) based on patterns learned on existing data [9]. This has enabled the field of generative AI to become useful in various fields of healthcare, including clinical diagnostics and customized medicine, research and administrative optimization.

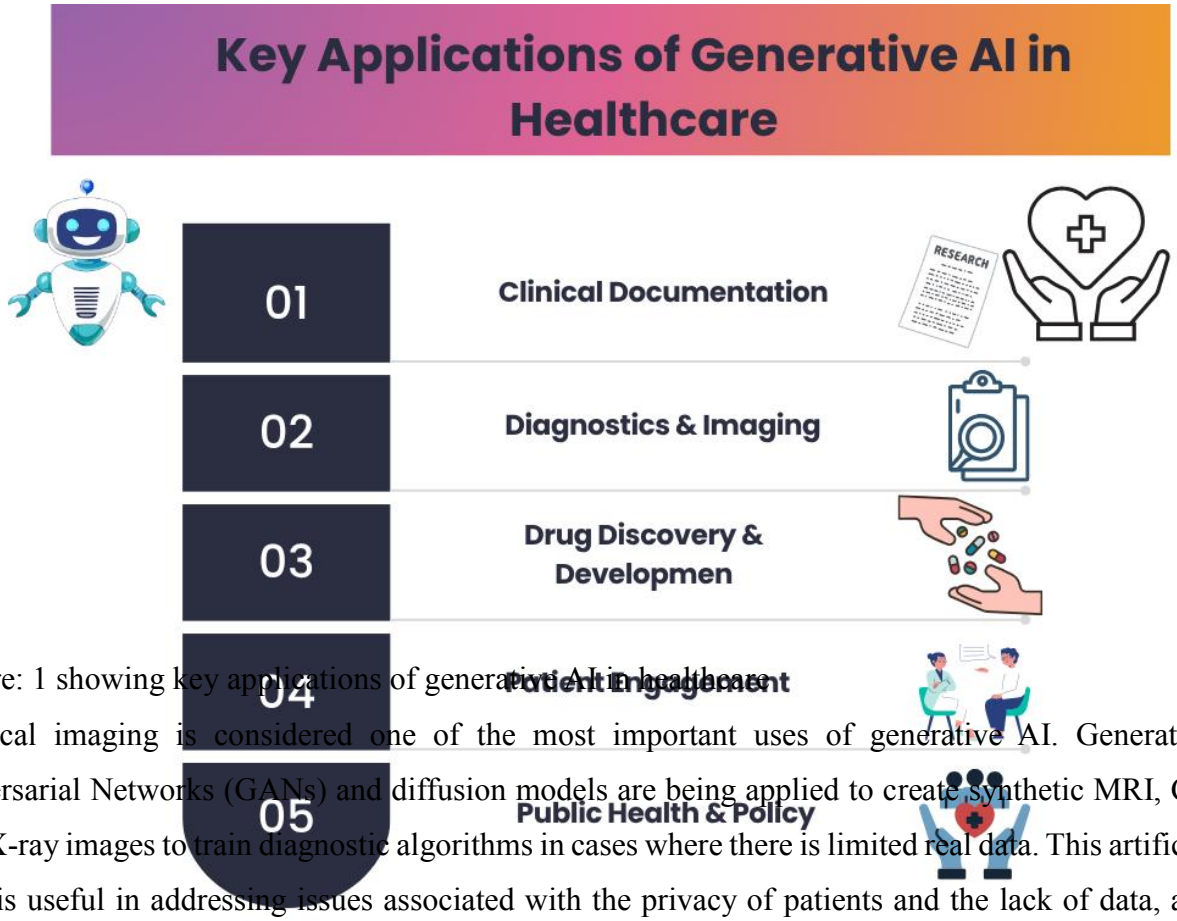


Figure: 1 showing key applications of generative AI in healthcare

Medical imaging is considered one of the most important uses of generative AI. Generative Adversarial Networks (GANs) and diffusion models are being applied to create synthetic MRI, CT, and X-ray images to train diagnostic algorithms in cases where there is limited real data. This artificial data is useful in addressing issues associated with the privacy of patients and the lack of data, and increases the robustness and accuracy of the model [10]. In a similar vein, generative models can be used in drug discovery and genomics to generate novel molecular compounds, model protein folding and anticipate drug-target interactions much faster than in a laboratory. It not only makes research faster but also makes it cheaper to develop, and less risky than experimenting with the product at an early stage [11].

In clinical practice, large language models (LLM) and other text-based generative systems can help

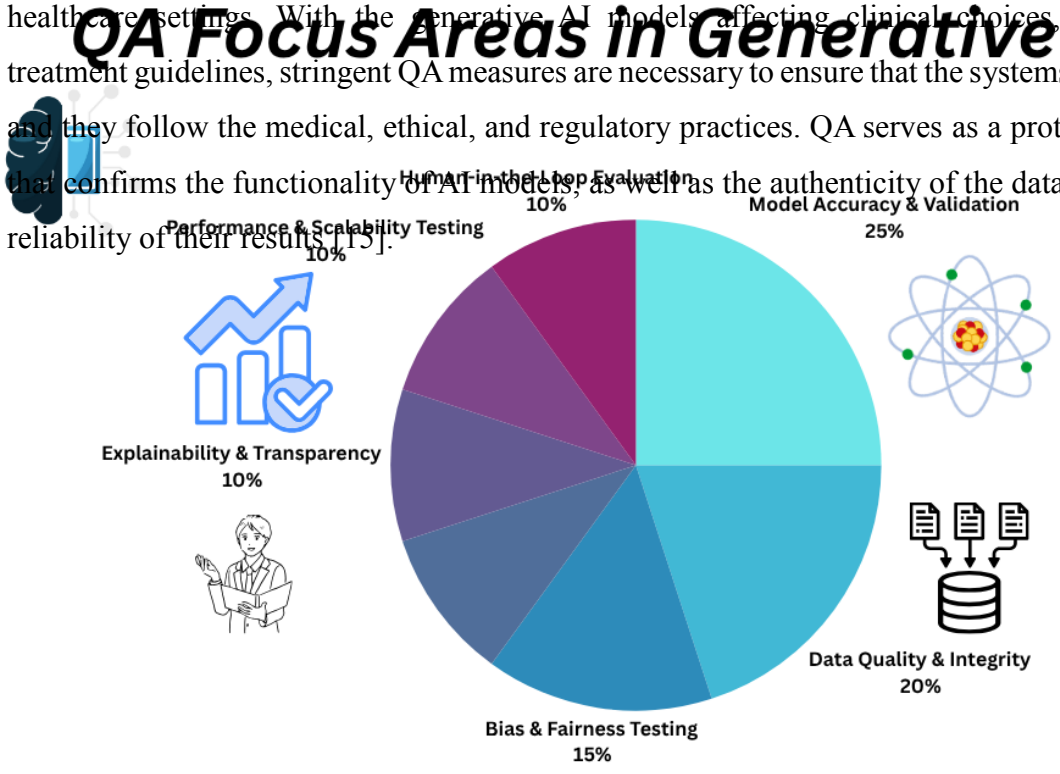
ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

health practitioners by summarizing patients, writing reports automatically, and helping make decisions based on context-specific suggestions. These models are able to extract insights and trends by evaluating large amounts of electronic health records (EHRs) and medical literature and clinical notes that can help to make more accurate and timely interventions. Virtual health assistants, predictive analytics and patient education are also and are being pursued using generative AI to improve access and personalization of medical provision [12].

Nevertheless, introducing generative AI in healthcare is associated with ethical, regulatory, and technical issues. The dependency on bulk data implies the threat of bias, data leaking, and misinformation. Although synthetic data can be helpful, it has to be thoroughly validated to be representative of diverse real-world and clinical applicability [13]. Transparency and explain ability, as well as strict validation procedures of AI-based medical devices, are now emanated as a priority by the regulatory agencies, including FDA and EMA. To make sure that generative AI systems are successfully and reliably adopted, it is important that they adhere to the standards of healthcare and the ethical principles. Generative AI, in a way, has immeasurable potential in changing the healthcare system by innovating, becoming efficient, and personalized. Nonetheless, to achieve its potential, a balanced approach that incorporates a robust method of quality assurance, ethical governance, and cyber defense and ensure safety, reliability, and trust in society is necessary [14].

Quality Assurance (QA) in Generative AI Systems

The concept of Quality Assurance (QA) of the generative AI systems is one of the underlying factors that guarantee the reliability, accuracy, and safety of these systems, especially when they are used in healthcare settings. With the generative AI models affecting clinical choices, diagnostics, and treatment guidelines, stringent QA measures are necessary to ensure that the systems work as intended and they follow the medical, ethical, and regulatory practices. QA serves as a protective mechanism that confirms the functionality of AI models, as well as the authenticity of the data they use and the reliability of their results [15].



ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

Figure: 2 showing QA focus areas in generative AI

In healthcare, data quality management is the starting point of QA because the performance of generative models is directly related to the data they are being trained on. The datasets should be exhaustive, representative and should be devoid of errors or biases that may translate to false findings or discriminative findings [16]. The anonymization and data preprocessing along with validation are thus vital in terms of ensuring the ethical compliance as well as technical soundness. Quality checks and continuous data auditing will aid in ensuring that the models change as the medical knowledge and demographic changes [17].

In addition to the data quality, the QA includes the model validation and verification. Validation is the process of assuring that a model achieves its intended clinical goal- be it the production of synthetic images, risk prediction of a disease or even the summation of patient data- whereas verification is the process of ensuring the system is running by its design requirements [18]. Outputs are evaluated using performance measures like accuracy, sensitivity, specificity, precision and recall. Also, stress testing and scenario assessment may be used to determine the limitations of the model in various clinical scenarios. This will enable the healthcare professionals to develop trust in AI-generated findings and reduce the chances of misdiagnosis [19].

Bias detection and ethical assurance is also another significant aspect of QA in generative AI. Since AI models are trained based on historical data, they may recreate systemic biases within the healthcare data. Using fairness measures, explain ability systems, and interpretability models will guarantee that output has transparency, traceability, and clinical explain ability. Additionally, the regulatory compliance with such standards as ISO 13485 (regarding medical equipment), FDA regulations on AI/ML systems, and GDPR on privacy issues should be considered as a form of QA [20].

Lastly, QA is not a single process but it is a lifecycle activity that is undertaken on a continuous basis and entails monitoring, retraining and auditing of AI systems. With the introduction of QA at each step of model development and deployment, healthcare organizations will be able to gain greater reliability, reduce risks, and learn to trust generative AI technologies to be as safe as innovations can be and with integrity in their principles [21].

Hacking Defense in Artificially Intelligent healthcare

With the rise in the implementation of AI technologies in healthcare systems, and especially generative AI models, cyber defense has become a significant element in the context of promoting patient safety, data integrity, and system reliability. Cyber-attacks are a very appealing target to the

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

healthcare industry because of the high price of medical information and the possible consequences of the attacks on human life [22]. The introduction of AI brings with it other areas of vulnerabilities such as manipulation of the model or data intrusion, which must be defended against with specific methods. AI-based healthcare cyber defense is therefore based on protecting all the layers of the AI ecosystem, including the acquisition and training of data as well as the deployment and utilization of AI systems [23].

Among the most frightening risks is a data pipeline attack. Given that generative AI is based on massive datasets, malicious actors can also use the technique of data poisoning to introduce false or misguided data into the training set, poisoning model behavior. This may lead to wrong diagnoses, misrepresentation, or distortion of records of the patients. On the same note, model inversion and membership inference attacks are trying to steal sensitive data about patients out of trained AI models, which endangers confidentiality and breaches privacy laws such as HIPAA and GDPR. Encryption, differential privacy, and data safe storage should be introduced during the AI lifecycle to overcome these threats [24].

Adversarial attacks, which involve small, invisible manipulations to medical data (e.g., medical images or lab results) with the aim of fooling AI systems, are another threat that is increasingly getting dangerous. An example of this is an attacker may make minor changes to a CT scan and this will make a model identify a tumor as harmless. To counter such attacks, a strong adversarial training, continuous threat modeling and anomaly detecting systems that can identify and inhibit suspicious patterns in real-time are required [25].

Along with technical protection, regulatory and compliance control is also a crucial aspect of healthcare cybersecurity. The guidelines on a secure approach to data management, control over data access, and responding to incidents are set by such standards as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and NIST cybersecurity framework. Healthcare facilities should also have a robust identity management, multi-factor authentication and network segmentation to reduce the probability of internal and external threats [26].

After all, it is not just AI in healthcare cyber defense that involves preventing attacks but it is also resilience. This consists of real-time threat intelligence and continuous monitoring, collaboration between cybersecurity professionals, clinicians, and AI developers, cross-disciplinary collaboration. Incorporating strong cyber defense into AI-based solutions will enable healthcare organizations to win the trust of patients, facilitate the continuation of their operations, and establish a secure base in the future in the field of generative AI innovations [27].

Global Insights in Artificial Intelligence and Computing
ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

Integrating QA and Cyber Defense Frameworks

Quality Assurance (QA) and Cyber Defense frameworks are to be integrated in order to develop trustworthy, safe, and efficient generative AI systems in healthcare. Although QA is aimed at accuracy, reliability, and adherence to the clinical standards, Cyber defense protects systems against threats, unauthorized access and data breaches [28]. Together, these frameworks form a single solution, which not only assures the functionality of AI applications but also safeguards the infrastructure supporting it, as well as the integrity of the data, which is of vital importance in healthcare settings where patient safety and privacy are the top priorities [29].

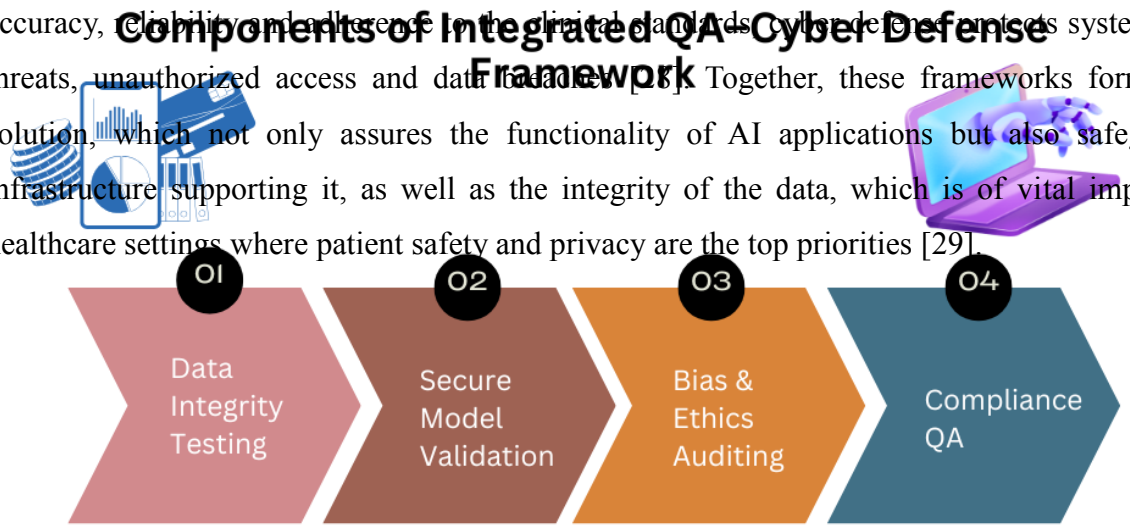


Figure: 3 showing components of integrated QA cyber defense framework

An additional element of this integration is that it has created a Secure Model Development Lifecycle (SMDLC), which is a unification of QA and cybersecurity principles in the AI development process. These stages of this lifecycle are secure data acquisition, proven preprocessing, constant validation, and real-time monitoring activities. On every level, QA mechanisms are used to ensure that the system performs to the desired standard and ethical level, and cyber defense measures are used to ensure that vulnerabilities can be identified and addressed prior to deployment. Indicatively, data quality and bias reduction are checked by QA during model training whereas model theft and data poisoning are countered by cyber defense [30].

Integrated governance and risk management are also another strength to this integration. The healthcare organizations may establish centralized supervision committees or structures that integrate the quality metrics with the security procedures, to achieve consistent evaluation of all the AI systems. This type of governance facilitates the adherence to international standards, namely ISO 27001 on information security and ISO 13485 on the management of quality of medical devices [31]. Automated monitoring of the deviations of quality performance and security posture can be performed via integrated auditing tools, and the best mitigation of risks can be implemented proactively [32].

Persistent enhancement is critical towards maintaining the incorporation of QA and cyber defense.

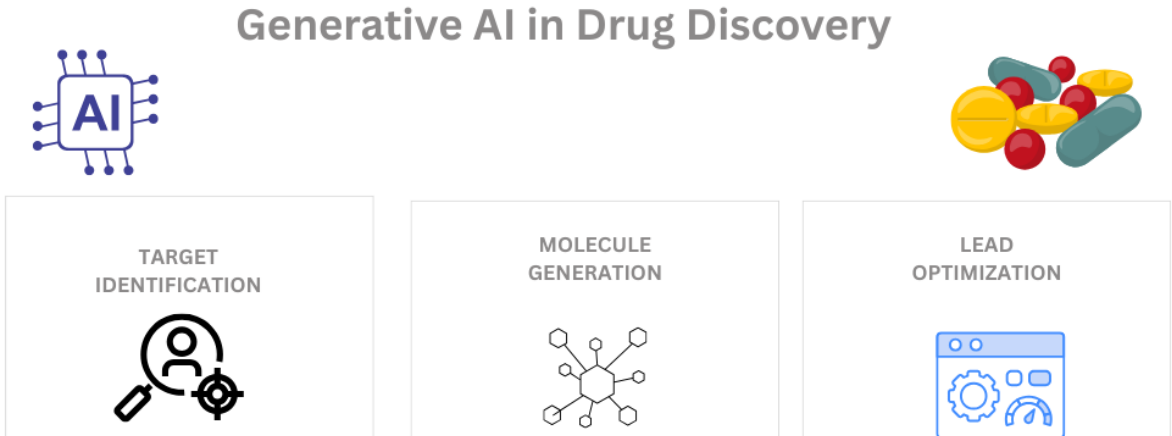
ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

System resilience is improved by regular audits, retraining verified data models, as well as incident response simulations. Healthcare organizations will be able to balance between innovation and safety by integrating QA and cybersecurity principles through all levels of generative AI, namely, data input and clinical output. This combined framework helps create a patient-trusting environment, avert regulations, and establish the base that will allow AI-based healthcare to be not only smart but also safe in the future [33].

Case Studies and Practical Applications

The real-life examples indicate that introducing quality assurance (QA) and cyber defense in generative AI will be able to change the healthcare systems without compromising safety, reliability, and data security. These applications demonstrate the practical issues and efficacy of the responsible application of generative AI in various medical fields like radiology, drug discovery and clinical data management [34]. The most notable example is the application of generative AI in medical imaging. Generative adversarial network (GAN) and diffusion models have been implemented in hospitals and research institutions to generate realistic MRI or CT images to be used to train diagnostic algorithms. As an example, QA systems guarantee that such synthetic images are up to clinical accuracy standards, by comparing them to real patient scans and checking that the diagnostic characteristics are obtained. In the meantime, the real and the synthetic datasets are safeguarded against tampering or unauthorized usage by integrated cyber defense mechanisms, like encryption and secure access controls. The two-layer strategy will be used to guarantee that AI systems are both efficient and safe and minimize misdiagnosis or manipulation of data [35].

A second example is drug discovery with the help of generative AI. Pharmaceutical firms are using AI to develop novel molecule structures, forecast protein-protein interactions, and streamline possible drug prospects. Under such circumstances, QA can be used to make sure that generated molecules comply with the biochemical feasibility and regulatory criteria, and the cyber defense can be used to ensure that proprietary datasets and the model parameters are not stolen or attacked by adversaries. An integrated QA-cybersecurity system assists in preserving the integrity of data, trade secrets, and improving the credibility of AI-based drug candidates [36].



ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

Figure: 4 showing generative AI in drug discovery

Clinical documentation and patient record synthesis Generative AI is also applied to clinical summaries or patient discharge notes, with large language models (LLMs) producing them. The factual accuracy and consistency of these AI-generated documents are ensured by QA systems, whereas compliance with the law of data protection, such as HIPAA and GDPR, is guaranteed by anonymization, encryption, and access control. This mixture has resulted in quicker documentation processes and additional data accuracy without jeopardizing the privacy of the patient [37].

Some of the lessons that have been learnt during these implementations include the value of constant validation, interdisciplinary cooperation, and openness. By incorporating quality assurance and cyber defense during the initial phases of AI development, the risks are reduced to a minimum, and the trustworthiness of stakeholders is established. Finally, these case studies have shown that once quality and security are viewed as inseparable variables, generative AI can generate safe efficient responsible innovations that enhance the robustness and reliability of the health care systems of today [38].

Challenges and Research Gaps

Although the applicability of generative AI in healthcare has a promising future, the implementation of quality assurance (QA) and cyber defense frameworks is accompanied by multiple challenges and gaps in the research. Such problems are based on the complexity of AI systems, the dynamism of healthcare data, and the ever-changing environment of cybersecurity threats. These issues need to be comprehended to build more resilient, transparent, and ethical healthcare systems based on AI [39].

Technical complexity is one of the most important problems. Generative AI models (including large language models (LLMs), generative adversarial networks (GANs), and diffusion models) have a tendency to be black boxes, which is why it is challenging to understand how these systems make decisions. Such a lack of explain ability makes QA difficult since it would be difficult to determine how models produce particular outputs and whether they are clinically valid [40]. In addition, there is an extreme heterogeneity of healthcare datasets, which contain text, imaging, genomic, and sensor data. Harmonizing and ensuring a consistent quality of data across these different inputs is the key obstacle to successful QA and model validation [41].

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

The other significant issue is security vulnerabilities peculiar to AI systems. In comparison to conventional IT-based infrastructures, AI models may be compromised by adversarial inputs, model inversion, data poisoning, and others. The current cybersecurity systems are not well prepared to identify or prevent such threats that are AI-specific. The current research is scarce in implementing adaptive, AI-conscious defense mechanisms that will be able to detect and prevent malicious manipulations without degrading the performance of the models [42]. Besides, the overall cybersecurity during the lifecycle of AI, including data collection, deployment, etc., also presupposes highly developed monitoring tools enabling to identify anomalies in real-time that are yet to be developed in the existing healthcare systems [43].

Ethically and legally, the inclusion of QA and cyber defense has issues with regulation and governance as well. In the healthcare industry, there are rigorous privacy regulations including HIPAA and GDPR, and the absence of international, widely accepted approaches to AI regulation makes it an uneven norm. One of the urgent research requirements is to develop universal standards of auditing, certification, and risk assessment of AI systems [44]. The absence of multidisciplinary collaboration and workforce preparedness gap exists. The gap that exists between clinicians, AI engineers, and cybersecurity professionals should be bridged to implement it successfully. Human-in-the-loop models of QA and explainable AI frameworks to increase trust and transparency should also be studied [45]. To overcome these issues, it is necessary to conduct constant innovations, align the regulations, and do research together. Only due to such efforts, the healthcare sector will be able to capitalize on the potential of generative AI to its full extent and remain safe, equitable, and secure [46].

Trends and Opportunities in the Future

The next part of the behavior of generative AI in healthcare is the creation of systems that are not only intelligent and efficient but also transparent, secure, and ethically oriented. Since the convergence between Quality Assurance (QA) and Cyber Defense is still a developing concept, a number of new trends and opportunities are defining how these technologies would shape to address the increasing needs of healthcare systems today. These advancements will improve the patient outcomes, increase the data security, and facilitate sustainable innovation within both clinical and research settings [47].

Among the most important future trends that can be identified is the use of federated learning and privacy-preserving AI. Conventional AI training involves data concentration in a single place, which promotes issues of privacy and heightens cybersecurity threats. In federated learning, the models can be trained in hospital systems without any sensitive information being transferred to a central server

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

[48]. This strategy is not only effective in complying with privacy laws like the HIPAA and GDPR, but it also contributes to an elevated level of data security with the help of decentralized architectures. Federated systems coupled with the QA practice can ensure the integrity of the information and constantly enhance the model performance in the context of various healthcare institutions [49].

The other area of up-and-coming interest is the creation of explainable and credible AI-systems. The next generation of AI generators will require justifications of their work so that clinicians can interpret and confirm AI-based recommendations. Making QA models explainable allows increasing the level of transparency in the model and reducing the risk of bias or inaccuracy affecting clinical decisions prior to their effect. Explainable AI will also play an important role in the regulation approval activities, with accountability and clinician trust in automated systems [50].

Another healthcare cybersecurity frontier is the integration of security mechanisms resistant to quantum attacks. With the development of quantum computing, the current encryption processes can be sensitive. The use of post-quantum cryptography and AI-based anomaly detection will be used proactively to protect sensitive medical information in the future. The studies on this topic are directed at developing AI systems that can be resilient and adapt to the changing cyber threats [51]. Human-AI collaboration will be given more focus in the future. Generative AI is becoming a companion and not a substitute of the medical worker, which will help in the diagnosis, treatment plan and communication with patients. The outcome of this cooperation backed with built-in QA and cybersecurity will be improved efficiency and trust. Secure, explainable, and collaborative systems characterize the future of generative AI in healthcare. Such improvements will open the way to a more intelligent, transparent and resilient healthcare ecosystem that will focus on both innovation and patient safety [52].

Conclusion

The implementation of Quality Assurance (QA) and Cyber Defense of generative AI applications is an important move towards creating secure, reliable, and ethically sound healthcare systems. With the ever-growing revolution in medical diagnostics, treatment planning, patient handling, and research, the need to develop strong frameworks that guarantee safety, accuracy, and trust is now more than ever. The conclusion of this review highlights that the future of AI in healthcare is not only based on technological innovation but also on the capacity to ensure a high level of quality control and high-level protection of cybersecurity across the entire lifecycle of AI.

Generative AI has massive potentials in changing healthcare delivery. It is able to create medical images, create realistic patient data to be used in training models, drug discovery, and even help in clinical documentation. These benefits have major responsibilities though. To train AI models,

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

healthcare organizations should make sure that the data they make the models is correct, not biased, and reflects patient demographics. This is the point of quality assurance. QA will guarantee that the outputs of AI are clinically meaningful and that the models comply with ethical and regulatory standards through systematic testing and validation and verification. Quality assurances are also capable of increasing transparency so that healthcare professionals can read and believe AI-generated insights instead of viewing them as black box suggestions.

At the same time, the growing reliance on digital systems and integrated healthcare equipment have intensified the risks of cybersecurity. Adversarial attacks, data poisoning, and model inversion are unique risks to generative AI systems, which may cause disastrous outcomes when unaddressed. Cyber defense mechanisms, in turn, also occupy a very important position. Healthcare institutions can protect patient data and integrity of AI models by applying encryption, secure access controls, constant monitoring, and detection of anomalies. Moreover, the adherence to legal regulations including HIPAA, GDPR and ISO requirements should be part of all phases of AI implementation to avoid abusing information and have confidence in patients.

When QA and cyber defense collide, it develops a multisided system of responsible AI governance. They are all united in the formation of a system in which quality, security and ethics are balanced. An integrated mode of governance may harmonize both the quality metrics and security measures where AI systems do not only work well but also operate in secure and compliant mode. Such integration promotes proactive risk management, vulnerability early detection, and continuous improvement, which are fundamental aspects of ensuring system resilience.

Nevertheless, the vision needs to be fulfilled in a number of steps that are prioritized. Standardized structures and benchmarks to AI validation and healthcare cybersecurity are required. The cooperation of policymakers, healthcare establishments, and developers of AI on an international level will assist in creating typical standards of QA and data protection. Furthermore, they should invest in employee education to close the knowledge gap in clinicians or AI engineers and cybersecurity professionals. The interdisciplinary education will monitor the fact that healthcare professionals will be able to use and supervise AI tools responsibly in practice.

In the future, transparency, explain ability, and accountability will become more significant in the future of generative AI in healthcare. Federated learning, explainable AI, and quantum-resistant security are designed to provide opportunities that can help in overcoming existing constraints. With the innovations of these technologies, it will help healthcare organizations to take advantage of AI in a safe and effective way and safeguard patient rights and public trust.

To sum up, there is no technical need to integrate QA and cyber defense, but an ethical one. It will

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

make certain that generative AI becomes an ally to the healthcare industry, and not a substitute to human experience. The healthcare sector can maximize the potential of generative AI by focusing on quality, security, and governance and provide safer, smarter, and more equitable medical care to everyone.

References

[1]. Qurashi SN, Sobia F, Hetany WA, Sultan H. Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. Medinformatics. 2025 Mar 24.

[2]. Nadeem G, Khaliq A, Ahmed J, Aziz A. Healthcare Security Challenges Leveraging Generative AI to Transform Cybersecurity. InNavigating Cyber Threats and Cybersecurity in the Software Industry 2025 (pp. 205-250). IGI Global Scientific Publishing.

[3]. Sallam M, Al-Mahzoum K, Sallam M. Generative Artificial Intelligence and Cybersecurity Risks: Implications for Healthcare Security Based on Real-life Incidents. Mesopotamian Journal of Artificial Intelligence in Healthcare. 2024 Dec 12;2024:184-203.

[4]. Chen Y, Esmaeilzadeh P. Generative AI in medical practice: in-depth exploration of privacy and security challenges. Journal of Medical Internet Research. 2024 Mar 8;26:e53008.

[5]. Paraschiv EA, Cîrnu CE, Vevera AV. Integrating artificial intelligence and cybersecurity in electronic health records: Addressing challenges and optimizing healthcare systems. InElectronic Health Records-Issues and Challenges in Healthcare Systems 2024 Dec 3. IntechOpen.

[6]. Andreoni M, Lunardi WT, Lawton G, Thakkar S. Enhancing autonomous system security and resilience with generative AI: A comprehensive survey. IEEE Access. 2024 Aug 6;12:109470-93.

[7]. Intaratat K, Lomchavakarn P, Boonsawad P, Boonsiri K, Kantaboon K, Intaratat D, Kumar R. Innovations in Smart Healthcare: Integrating Generative Artificial Intelligence with Federated Learning. InGenerative Artificial Intelligence in Healthcare (pp. 224-246). CRC Press.

[8]. Kabeer MM. AI for Smarter Product Development and Manufacturing. Global Journal of Universal Studies. 2025 Jun 6;2(1):134-53.

[9]. Teo ZL, Quek CW, Wong JL, Ting DS. Cybersecurity in the generative artificial intelligence era. Asia-Pacific Journal of Ophthalmology. 2024 Jul 1;13(4):100091.

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

[10]. Mohawesh R, Ottom MA, Salameh HB. A data-driven risk assessment of cybersecurity challenges posed by generative AI. Decision Analytics Journal. 2025 Jun 1;15:100580.

[11]. Shah IA, Sial Q, Fateh S, editors. Generative AI Techniques for Sustainability in Healthcare Security. IGI Global; 2024 Dec 2.

[12]. Rabbani SA, El-Tanani M, Sharma S, Rabbani SS, El-Tanani Y, Kumar R, Saini M. Generative artificial intelligence in healthcare: applications, implementation challenges, and future directions. BioMedInformatics. 2025 Jul 7;5(3):37.

[13]. Ahmad I, Nasim F, Khawaja MF, Naqvi SA, Khan H. Enhancing IoT security and services based on generative artificial intelligence techniques: a systematic analysis based on emerging threats, challenges and future directions. Spectrum of engineering sciences. 2025 Jan 23;3(2):1-25.

[14]. Maddali R. SYNTHETIC DATA GENERATION FOR QUALITY ASSURANCE IN LARGE-SCALE AI MODELS. International Journal of Engineering Technology Research & Management (IJETRM). 2024;8(07).

[15]. Kabeer MM. AI in Product Management: Efficiency, Quality, and Innovation. Global Journal of Universal Studies. 2024 Dec 16;1(2):165-85.

[16]. Bala I, Pindoo I, Mijwil MM, Abotaleb M, Yundong W. Ensuring security and privacy in Healthcare Systems: a Review Exploring challenges, solutions, Future trends, and the practical applications of Artificial Intelligence. Jordan Medical Journal. 2024 Jul 15;58(3).

[17]. Balasubramanian P, Liyana S, Sankaran H, Sivaramakrishnan S, Pusuluri S, Pirttikangas S, Peltonen E. Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. Artificial Intelligence Review. 2025 Nov;58(11):1-34.

[18]. Veluru CS. Impact of artificial intelligence and generative AI on healthcare: security, privacy concerns and mitigations. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-364. DOI: doi. org/10.47363/JAICC/2024 (3). 2024;347:2-6.

[19]. Al-Hammuri K, Gebali F, Kanan A. ZTCloudGuard: Zero trust context-aware access management framework to avoid medical errors in the era of generative AI and cloud-based health information ecosystems. AI. 2024 Jul 8;5(3):1111-31.

[20]. Kabeer MM. Artificial Intelligence in Modern Manufacturing: Opportunities and Barriers. Global Trends in Science and Technology. 2025 Jul 16;1(3):83-100.

[21]. Dhoni PS, Kumar R. Synergizing generative Artificial Intelligence and cybersecurity: Roles of generative Artificial Intelligence entities, companies, agencies and government in enhancing cybersecurity. Journal of Global Research in Computer Sciences. 2023;14(3).

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

[22]. Wang Y, Liu C, Zhou K, Zhu T, Han X. Towards regulatory generative AI in ophthalmology healthcare: a security and privacy perspective. British Journal of Ophthalmology. 2024 Oct 1;108(10):1349-53.

[23]. Ustymenko S, Phadke A. Promise and challenges of generative AI in healthcare information systems. InProceedings of the 2024 ACM southeast conference 2024 Apr 18 (pp. 223-228).

[24]. Yu P, Xu H, Hu X, Deng C. Leveraging generative AI and large language models: a comprehensive roadmap for healthcare integration. InHealthcare 2023 Oct 20 (Vol. 11, No. 20, p. 2776). MDPI.

[25]. Nadella GS, Addula SR, Yadulla AR, Sajja GS, Meesala M, Maturi MH, Meduri K, Gonaygunta H. Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management. Computers. 2025 Feb 8;14(2):55.

[26]. López Delgado JL, López Ramos JA. A Comprehensive Survey on Generative AI Solutions in IoT Security. Electronics. 2024 Dec 17;13(24):4965.

[27]. Yigit Y, Ferrag MA, Sarker IH, Maglaras LA, Chrysoulas C, Moradpoor N, Janicke H. Critical infrastructure protection: Generative AI, challenges, and opportunities. arXiv preprint arXiv:2405.04874. 2024 May 8.

[28]. Huang K, Wang Y, Goertzel B, Li Y, Wright S, Ponnapalli J. Generative AI Security. Future of Business and Finance. 2024.

[29]. Kabeer MM. Next-Generation Food Manufacturing: AI as a Catalyst for Productivity and Quality Enhancement. Global Food Research. 2025 Jul 15;1(1):1-8.

[30]. Miran S, Siraj M, Mumtaz M, Khan N, Rehman A. Transforming healthcare security and sustainability through pioneering generative AI solutions. Generative AI Techniques for Sustainability in Healthcare Security. 2025:331-48.

[31]. Khinvasara T, Ness S, Shankar A. Leveraging AI for enhanced quality assurance in medical device manufacturing. Asian Journal of Research in Computer Science. 2024 Apr 8;17(6):13-35.

[32]. Qureshi KN, Nafea H, Kim P. Advancing healthcare systems: A tri-tier architecture by using data communication, AI data generative and regulation and compliance standards. Expert Systems. 2025 Feb;42(2):e13742.

[33]. Mala DJ, Dhanapal AC, Sthapit S, Khadka A. Integrating AI Techniques into the Design and Development of Smart Cyber-Physical Systems: Defense, Biomedical, Infrastructure, and Transportation. CRC Press; 2025 Jun 30.

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

[34]. Aung YL, Christian I, Dong Y, Ye X, Chattopadhyay S, Zhou J. Generative ai for internet of things security: Challenges and opportunities. arXiv preprint arXiv:2502.08886. 2025 Feb 13.

[35]. Tallam K. Engineering Risk-Aware, Security-by-Design Frameworks for Assurance of Large-Scale Autonomous AI Models. InProceedings of the Future Technologies Conference 2025 Oct 16 (pp. 209-227). Cham: Springer Nature Switzerland.

[36]. Nankya M, Mugisa A, Usman Y, Upadhyay A, Chataut R. Security and privacy in E-health systems: a review of AI and machine learning techniques. IEEE Access. 2024 Sep 27.

[37]. Kabeer MM. AI in Quality Assurance: A Systematic Review. Global Research Repo. 2025 Oct 21;1(3):117-37.

[38].]Oniani D, Hilsman J, Peng Y, Poropatich RK, Pamplin JC, Legault GL, Wang Y. Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare. NPJ Digital Medicine. 2023 Dec 2;6(1):225.

[39]. Kabeer MM. Utilizing Machine Learning for Continuous Process Improvement in Lean Six Sigma. Global Trends in Science and Technology. 2025 May 7;1(2):49-63.

[40]. Khan A, Jhanjhi N, Abdulhabeb GA, Ray SK, Ghazanfar MA, Humayun M. Securing IoT Devices Using Generative AI Techniques. InReshaping CyberSecurity with Generative AI Techniques 2025 (pp. 219-264). IGI Global.

[41]. Rahman MA, Al-Hazzaa S. Next-Generation Virtual Hospital: Integrating Discriminative and Large Multi-Modal Generative AI for Personalized Healthcare. InGLOBECOM 2024-2024 IEEE Global Communications Conference 2024 Dec 8 (pp. 3509-3514). IEEE.

[42]. Kabeer MM. Automation Meets Accuracy: A Deep Dive into AI for Quality Assurance. Global Research Repo. 2025 Oct 25;1(3):138-56.

[43]. Yigit Y, Buchanan WJ, Tehrani MG, Maglaras L. Review of generative ai methods in cybersecurity. arXiv preprint arXiv:2403.08701. 2024 Mar 13.

[44]. Sammangi H, Jagatha A, Liu J. Harnessing Generative AI and Large Language Models for Revolutionizing Cybersecurity in the Internet of Things: Ethical and Privacy Implications.

[45]. Ferrag MA, Alwahedi F, Battah A, Cherif B, Mechri A, Tihanyi N. Generative ai and large language models for cyber security: All insights you need. Available at SSRN 4853709. 2024 Jan 1.

[46]. Chugh H. Cybersecurity in the age of generative AI: Usable security & ThreatGPT. Int. J. Res. Appl. Sci. Eng. Technol. 2023 Oct;12:1-1.

[47]. Nott C. Organizational Adaptation to Generative AI in Cybersecurity: A Systematic Review. arXiv preprint arXiv:2506.12060. 2025 May 31.

ISSN : 3079-6830
Volume 1, Number 3, 2025
https://doi.org/10.70445/giaic.1.3.2025.75-91

[48]. Oloyede J, Owen J. Enhancing Data Quality and Integrity with AI: A Deep Learning Perspective Author: Joseph Oluwaseyi, Fajinmi John. Fajinmi John (February 19, 2025). 2025 Feb 19.

[49]. Hasan M, Faruq MO. AI-Augmented Risk Detection in Cybersecurity Compliance: A GRC-Based Evaluation in Healthcare and Financial Systems. ASRC Procedia: Global Perspectives in Science and Scholarship. 2025 Apr 29;1(01):313-42.

[50]. Acuña EG. Healthcare cybersecurity: Data poisoning in the age of ai. Journal of Comprehensive Business Administration Research. 2024 Oct 17.

[51]. Ankalaki S, Rajesh AA, Pallavi M, Hukkeri GS, Jan T, Naik GR. Cyber attack prediction: From traditional machine learning to generative artificial intelligence. IEEE Access. 2025 Mar 3.

[52]. KO H, Ogiela MR. Security Strategy of Digital Medical Contents Based on Blockchain in Generative AI Model. Computers, Materials & Continua. 2025 Jan 1;82(1).