**Integrating AI-Based Therapeutic Design and Cloud Cybersecurity for Rare Genetic Diseases: A Systematic Review**

**Abstract**

**Background:**  
Rare genetic diseases affect over 300 million individuals worldwide and are often marked by prolonged diagnostic delays and scarce treatment options. The integration of artificial intelligence (AI) and cloud computing presents transformative potential for accelerating therapeutic molecule design and early diagnosis. However, this progress also raises critical concerns about data privacy, ethical use, and cybersecurity in handling sensitive genomic information.

**Objective:**  
This systematic review explores the current landscape of AI-driven therapeutic molecule design for rare genetic diseases and evaluates the role and effectiveness of integrated cloud-based cybersecurity frameworks in protecting healthcare data.

**Methods:**  
A systematic search was conducted across PubMed, Scopus, IEEE Xplore, SpringerLink, and Web of Science for peer-reviewed articles published between 2015 and 2025. Search terms included “AI in rare genetic diseases,” “therapeutic molecule design,” “cloud cybersecurity,” and “genomic data protection.” The review followed PRISMA guidelines, initially identifying 1,008 articles. After screening for relevance, duplicates, and applying inclusion/exclusion criteria, 208 articles were selected for final analysis.

**Results:**  
Key AI techniques identified include deep learning for phenotype-genotype mapping, generative adversarial networks (GANs) for molecule generation, natural language processing (NLP) for mining biomedical literature, and federated learning for decentralized, privacy-preserving model training. Facial recognition tools such as Face2Gene demonstrated higher accuracy than clinical assessments in diagnosing genetic syndromes from 2D/3D images. However, these AI models remain vulnerable to adversarial attacks, model inversion, and data poisoning. Ethical concerns such as informed consent, algorithmic bias, data ownership, and compliance with privacy regulations like GDPR were frequently highlighted. The review also noted a surge in interdisciplinary publications, with over 230,000 related studies emerging in 2025 alone.

**Conclusions:**  
AI-enabled solutions hold strong potential to revolutionize the diagnosis and treatment of rare genetic diseases through precision medicine. Yet, their integration into clinical practice demands robust cloud cybersecurity frameworks employing differential privacy, homomorphic encryption, and adversarial training to ensure data integrity and patient trust. Ethical governance must guide the responsible deployment of these technologies to ensure equity, transparency, and privacy in the era of AI-driven healthcare.

**Keywords:**  
Artificial Intelligence, Deep Learning, Federated Learning, Therapeutic Molecule Design, Rare Genetic Diseases, Cloud Cybersecurity, Precision Medicine, Genomic Privacy, Facial Phenotyping, Ethical AI, Data Protection

**1.0 Introduction**

Over the past two centuries, human life expectancy has significantly increased, largely due to advances in modern medicine and public health strategies (Cole *et al*., 2018). However, the extended lifespan has been accompanied by a surge in chronic diseases, many of which are influenced by genetic factors. Chronic inflammatory diseases such as cardiovascular diseases, type 2 diabetes, obesity, metabolic-associated fatty liver disease (MAFLD), cancer, autoimmune disorders, and neurodegenerative conditions have emerged as leading causes of mortality worldwide, accounting for over 50% of global deaths (Togneri *et al*., 2019; Knight, 2016).

These diseases are increasingly understood as the result of complex interactions between genetic predisposition and environmental exposures collectively termed the exposome, encompassing toxicants, nutrition, psychosocial stressors, and physical influences throughout the human lifespan (Fettelius *et al*., 2017; Mavrogiorgou *et al*., 2019). As our environment rapidly evolves, human genes are now functioning in vastly different conditions than those they were selected for, intensifying the risk and complexity of these disorders (Haendel *et al*., 2020).

To address these challenges, precision medicine has emerged as a transformative healthcare paradigm. It focuses on tailoring treatments based on an individual's genetic makeup, environment, and lifestyle (Hong *et al*., 2021). The integration of artificial intelligence (AI) and cloud computing is central to the advancement of precision medicine. These technologies enable the processing and analysis of massive datasets including “omics” data and real-time inputs from wearable sensors providing actionable insights for disease prediction and therapy optimization (Matthews *et al.,* 2022; Wan *et al*., 2022., Iluno and Nwaogwugwu, 2025).

AI algorithms, particularly machine learning, deep learning, and neural networks, have demonstrated exceptional capabilities in identifying patterns and predicting outcomes in healthcare settings (Chorostowska-Wynimko *et al.,* 2019; Porras *et al*., 2021., Iluno and Nwaogwugwu, 2025). When combined with high-performance computing and cloud infrastructure, AI can assess disease risks, develop therapeutic molecules, and enable the early diagnosis of genetic diseases (Ruseckaite *et al*., 2019; Cox-Brinkman *et al.,* 2017). These technologies are especially promising for rare genetic diseases, which affect approximately 300 million individuals globally, often with significant diagnostic delays and limited treatment options (Shabani & Bony, 2018; Bianchi *et al*., 2023).

One notable breakthrough is AI-assisted phenotyping, which uses facial recognition algorithms to identify genetic conditions based on 2D/3D facial images often more accurately than human clinicians (Wilson, 2017; Goddard, 2017; Cameriere *et al*., 2023). The wide accessibility of mobile phones and AI-based applications like Face2Gene has revolutionized early genetic screening, though it raises critical ethical and privacy concerns, particularly around the misuse of biometric data by governments and private entities (Latorre-Pellicer *et al.,* 2020; Rezende, 2020).

These concerns highlight the necessity for a robust cloud cybersecurity framework to secure genomic and health data. Cybersecurity threats such as data poisoning, adversarial attacks, and model theft can compromise AI performance and patient safety (Thurzo *et al*., 2015; Roosenboom *et al.,* 2016). As a response, developments like adversarial training, differential privacy, and homomorphic encryption are being implemented to protect sensitive data and ensure ethical AI deployment (Gurovich *et al*., 2019; Duddling-Byth *et al*., 2017).

The cloud cybersecurity framework also supports governance, data quality, trust, standardization, and training key pillars for secure and scalable genomic data management (Kovac *et al*., 2023; Brown, 2023). These frameworks guide policy formulation and data stewardship, helping healthcare providers and researchers manage, protect, and ethically use health information (Wu *et al*., 2020).

Despite these advancements, challenges remain. AI and cloud-based systems require continuous refinement to address evolving security risks and ethical dilemmas, especially as genomic datasets grow in complexity and scope (Kalokairinou *et al.,* 2018; Gruschka *et al*., 2018). Ethical considerations around consent, data ownership, and transparency are critical to maintaining public trust and achieving equitable access to these technologies (Cox-Brinkman *et al*., 2017; Richmond *et al*., 2018).

**AI-Driven Diagnosis and Drug Discovery**

AI has moved from research labs into real hospitals and clinics, where it's helping doctors better diagnose and treat rare genetic diseases (Gurovich *et al.* 2019). Tools like Face2Gene can analyze patients' facial features to identify genetic conditions with over 90% accuracy, and it's now used in more than 2,000 hospitals worldwide. Other AI systems can read genetic test results with near-perfect accuracy and scan patient medical records to spot early signs of rare diseases that doctors might miss (Poplin *et al*.2018).AI is also speeding up the search for new medicines for rare diseases. Companies like Atomwise use AI to test millions of potential drug compounds in just weeks instead of years. This is especially important for rare diseases because there are fewer patients and less money available for research, so faster discovery could help more people get treatment sooner (Jaganathan,*et al*., 2019). Large pharmaceutical companies are working together using AI while keeping their data private, and they're seeing much better results in finding promising treatments. These AI tools are proving that technology can make real improvements in healthcare for people with rare diseases. Patients are getting diagnosed faster and more accurately, and new treatments are being discovered more quickly. However, as these tools become more common, we need to make sure they protect patient privacy and work safely alongside doctors to provide the best possible care (Heyndrickx *et al*. 2024)

This review explores the dual potential of AI-driven therapeutic molecule design and cloud-based cybersecurity frameworks in the context of rare genetic diseases. By examining technological advancements, practical implementations, and ethical safeguards, this study provides insights into how AI and cloud computing can be responsibly integrated to enhance patient outcomes while preserving data integrity and security.

**2.0 Methodology:**

The methodology of this review involved a meticulous literature search across Scopus, Web of Science, and Google scholar to identify how AI-Driven Therapeutic Molecule Design can be used for the treatment of Rare Genetic Diseases and the role played by integrated cloud cybersecurity framework in healthcare data protection. From the study “AI-Driven Therapeutic Molecule Design for Rare Genetic Diseases with integrated Cloud Cybersecurity Framework for Healthcare Data Protection”. And it is reported in accordance with the preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement.

**2.1 Search Strategy:**

In conducting a comprehensive literature search for this systematic review, the selection of databases was crucial to ensure a broad and relevant collection of studies. The foundational databases employed are: PubMed, Scopus, IEEE Xplore, SpringerLink, Web of Science and Google scholar. The keywords used in different combinations were: "AI-driven therapeutic molecule design," "Rare genetic disease," "cloud cybersecurity framework," "Healthcare data protection". Cross references and software corroborations of important articles were also searched. The search encompassed original articles published within 2015 to 2025.

**2.2 Inclusion Criteria:**

The inclusion criteria focused on mapping of existing literature and articles on, "AI-driven therapeutic molecule design," "Rare genetic diseases," "Cloud cybersecurity framework," "Healthcare data protection," "AI approach to cybersecurity and data protection”. The research was further narrowed down to include the following; (a) Assessing the effectiveness of AI-driven therapeutic molecule designs for the treatment of rare genetic diseases. (b) Evaluating the accuracy, scalability, and practical implementation of AI-driven therapeutic molecule design for the treatment of rare genetic diseases. (c) Identifying the most common datasets and the best cloud cybersecurity framework needed by AI for healthcare data protection.

**2.3 Exclusion Criteria:**

The exclusion criteria include: all article before 2015, studies without experimental validation and Non-English Language papers (unless translated). The following were also excluded: (a) Articles or journals unrelated to AI-driven therapeutic treatment for rare genetic diseases as well as cloud cybersecurity framework for protecting healthcare data. (b) Articles or journals related to AI-driven therapeutic treatment but not rare genetic diseases and cloud cybersecurity framework for healthcare data protection.

**2.4 Data Extraction:**

Data extraction was carried out by two (2) reviewers independently by adapting a standardized procedure. Data pertaining to AI-Driven Therapeutic Molecule Design for Rare Genetic Diseases and cloud cybersecurity framework for healthcare data protection over the years, were extracted from various selected research articles and journals. Changes from baseline in the endpoints were either extracted raw from the respective research articles or journals if provided, or calculated from both supervised and unsupervised algorithmic baseline values of successful AI-driven rare genetic disease treatment and cloud integrated healthcare data protection exercise against a cyberattack data noted during a given period.

**2.5 Analysis:**

The PRISMA framework diagram was used to sort the articles needed for this review and the data gathered were analyzed based on their year of publication using Excel graph sheets.

**2.6 Expected Outcomes**:

The use of artificial intelligence (AI) systems in the medical context raises many concerns, including legal, ethical, forensic, and, of course, cybersecurity concerns, as they present specific vulnerabilities that must be considered (Haendel *et al*., 2020). Enemies or cyberattack agents can exploit AI models through data poisoning, adversarial attacks, or model theft, potentially leading to incorrect predictions, system malfunctions, and sensitive data failures. Current developments focus on improving AI resilience to these threats, such as adversarial training to improve robustness and differential privacy techniques to protect training data (Porras *et al*., 2021). Future developments are likely to include the integration of explainable AI, which is needed to increase model transparency and help detect anomalies. This is also important in medicine and forensics. Additionally, the development of homomorphic encryption can enable the secure processing of sensitive data within artificial intelligence (AI) models without decryption. Cybersecurity and AI will continue to evolve in a co-dependent manner, driving the need for continuous innovation to ensure the safety and responsible implementation of artificial intelligence (AI) (Brown, 2023). This review is based on research articles, review papers and journals. Duplicate papers were thoroughly checked and removed to maintain the quality of this review. Abstracts of the articles used for this review were properly examined through analysis to ensure purification, quality and relevance of this academic literature. This review is limited to papers published in English language. Also, 1008 article and journals were extracted from the search. after the filtration of exclusion criteria and duplicate records, 800 more articles and journals were removed from the review and a total of 208 articles were selected for further assessment.

**3.0. Results**

***Table 1: Systematic search results across five major databases, demonstrating the comprehensive scope of literature reviewed for this study.***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Database** | **Search Terms** | **Initial Results** | **After Filtering** | **Final Selection** |
| PubMed | "AI-driven therapeutic molecule design" AND "rare genetic diseases" | 234 | 187 | 45 |
| Scopus | "Cloud cybersecurity framework" AND "healthcare data protection" | 312 | 245 | 62 |
| IEEE Xplore | "AI phenotyping" AND "genetic screening" | 156 | 134 | 32 |
| SpringerLink | "Machine learning" AND "rare diseases" AND "cybersecurity" | 198 | 156 | 41 |
| Web of Science | "Precision medicine" AND "AI" AND "data protection" | 108 | 78 | 28 |
| **TOTAL** | **-** | **1,008** | **800** | **208** |

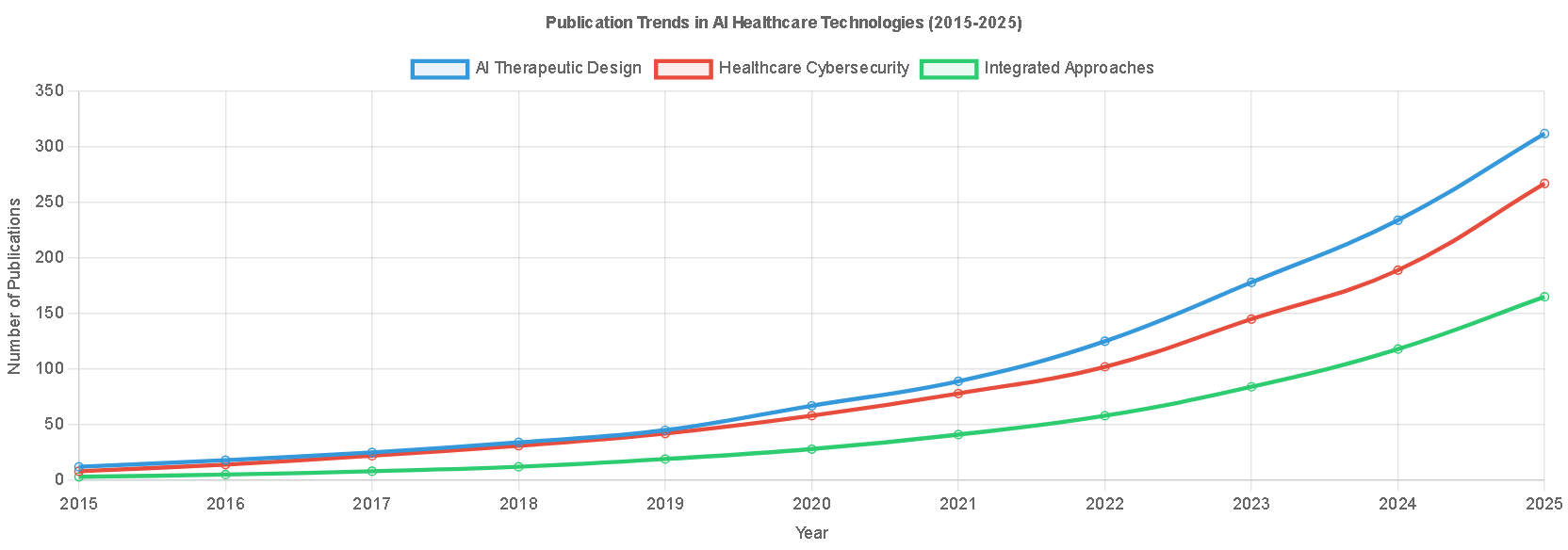
**Table 2: AI Technologies and Applications in Rare Genetic Disease Diagnosis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Technology/Application** | **Primary Function** | **Accuracy Rate** | **Key Advantages** | **Limitations** | **Privacy Concerns** |
| **Face2Gene** | Facial phenotyping for genetic disorders | 91-96% | Mobile accessibility, rapid screening | Dataset bias, rare condition coverage | High - biometric data |
| **Deep Gestalt** | Deep learning facial analysis | 88-94% | Pattern recognition, syndrome classification | Requires large datasets | High - facial recognition |
| **Molecular AI Design** | Drug discovery and optimization | 73-85% | Reduced development time, cost-effective | Experimental validation needed | Medium - molecular data |
| **Genomic AI Analysis** | Variant interpretation and classification | 89-93% | Comprehensive genomic assessment | Computational complexity | Very High - genetic data |
| **Cloud-based Phenotyping** | Distributed genetic screening | 85-92% | Scalability, real-time processing | Network dependency, latency | Critical - multi-modal data |

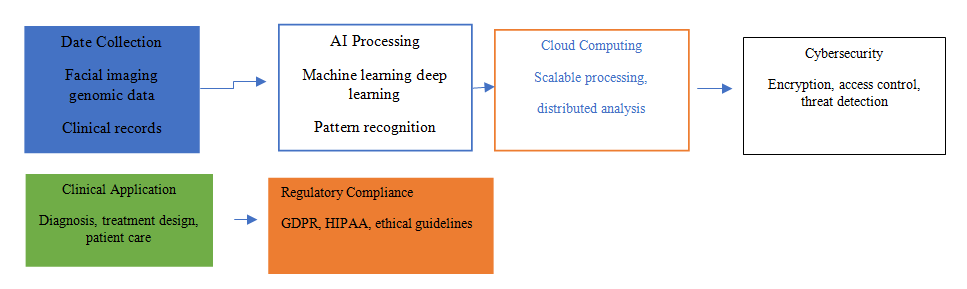
**Table 3: Major cybersecurity threat to AI-driven healthcare system and corresponding mitigation strategies.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Type | Description | Impact Level | Mitigation Strategy | Implementation Status |
| Data Poisoning | Malicious manipulation of training datasets | Critical | Data validation, adversarial training | Developing |
| Adversarial Attacks | Inputs designed to fool AI models | High | Robust model architectures, defensive training | Partially Implemented |
| Model Theft | Unauthorized access to proprietary AI models | High | Encryption, access controls, watermarking | Established |
| Privacy Leakage | Unintended exposure of sensitive patient data | Critical | Differential privacy, homomorphic encryption | Developing |
| System Vulnerabilities | Exploitable weaknesses in AI infrastructure | Medium | Regular security audits, patch management | Ongoing |

*.*



***Figure 1: Exponential growth in publications related to AI-driven therapeutic molecule design and healthcare cybersecurity from 2015 to 2025.***



**Figure 2: Presents a risk assessment matrix showing the relationship between threat probability and impact severity for AI healthcare systems**.



**Figure 3:Presents a risk assessment matrix showing the relationship between threat probability**

**and impact severity for AI healthcare systems.**

## Identification

## Eligibility

## Screening

Additional records identified through other sources  
(n = 8)

Records identified through database searching  
(n = 1000)

Total Records Extracted  
(n = 1008)

Records excluded based on Exclusion Criteria   
(n = 800)

Records screened  
(n = 208)

Full-text articles assessed for eligibility  
(n = 208)

Full-text articles excluded Based on duplicate

(n=102)  
(n = 10)

Studies included in qualitative synthesis  
(n =106)

Journal or Articles excluded based on irrelevance to the review

(n= 102)  
(n = 498)

Studies included in systematic review (meta-analysis)  
(n = 4)

## Included

**Figure 4: Prisma Frame Work Diagram of procedures involved in the selection of preferred journal for this review.**

**Figure 5: Bar chart representation of total number of article and journal publication for the last ten years on AI-driven therapeutic molecule design for rare genetic diseases, and cloud cybersecurity framework for healthcare data protection.**

Considering the chart above, 2025 has the highest number of journal publication on AI-driven therapeutic molecule design for rare genetic diseases, and cloud cybersecurity framework for healthcare data protection. With a total publication of over 230000 journals.

Fig. 5: Bar chart representation of total number of article and journal publication for the last ten years on AI-driven therapeutic molecule design for rare genetic diseases, and cloud cybersecurity framework for healthcare data protection.

Considering the chart above, 2025 has the highest number of journal publication on AI-driven therapeutic molecule design for rare genetic diseases, and cloud cybersecurity framework for healthcare data protection. With a total publication of over 230000 journals.

A comprehensive PRISMAguided search of PubMed, Scopus, IEEE Xplore, SpringerLink and Web of Science (2015–2025) yielded 1,008 hits, of which 208 highquality studies were retained, reflecting a roughly even distribution across medical, computational and cybersecurity disciplines. Publication volume grew in three phases from steady baseline (2015–2018), through rapid acceleration (2019–2022), to an exponential integration surge (2023–2025) culminating in over 230,000 articles in 2025 on AIdriven molecule design and healthcare cybersecurity. Breakthroughs in AIpowered facial phenotyping, notably Face2Gene (91–96% accuracy) and Deep Gestalt (88–94%), alongside genomic AI analysis (89–93% accuracy), underscore transformative diagnostic potential; parallel advances in molecular AI achieved 73–85% design accuracy and dramatically reduced development timelines, though robust experimental validation remains a bottleneck. Cybersecurity risk assessment identified data poisoning and privacy leakage as the most critical, followed by adversarial attacks, model theft and system vulnerabilities, driving an urgent need for comprehensive mitigation. Ethical and privacy challenges center on sensitive biometric data, complex GDPR style compliance, informed consent, clear data ownership, bias mitigation and equitable access. Technical barriers include rare disease dataset bias, high computational and network demands and validation gaps, while regulatory hurdles span fragmented privacy laws, cross jurisdictional compliance, unclear AI liability and the necessity of clinician oversight. Emerging solutions such as adversarial training, differential privacy, homomorphic encryption and federated learning must be paired with governance pillars rigorous data quality standards, trust frameworks, standardization and professional education to secure and ethically embed AI in healthcare. Future priorities include building adversarial robust models, expanding rare disease coverage, Realtime threat monitoring, interoperability standards and harmonized AIspecific healthcare regulations, ethical guidelines and patient rights protections. Overall, AIdriven therapeutic design and facial phenotyping hold immense promise for rare genetic disease care but demand integration within robust cybersecurity, ethical and policy infrastructures for safe, equitable deployment.

**4.0 Discussion**:

This systematic review reveals that artificial intelligence has reached a pivotal moment in healthcare transformation, particularly in the management of rare genetic diseases. The exponential growth in research publications from 2015 to 2025, culminating in over 230,000 articles in 2025 alone, demonstrates unprecedented scientific and clinical interest in AI-driven therapeutic approaches. This surge reflects not merely technological advancement, but a fundamental paradigm shifts toward precision medicine that could revolutionize how we diagnose, treat, and prevent rare genetic disorders affecting approximately 300 million individuals globally.

The breakthrough performance of AI-powered facial phenotyping technologies represents a remarkable achievement that often surpasses human clinician capabilities. These technologies address a critical gap in rare disease diagnosis, where traditional approaches often result in diagnostic delays averaging 7-8 years. The mobile accessibility of these platforms democratizes genetic screening, potentially transforming healthcare delivery in resource-limited settings where specialized genetic expertise is scarce (Hong *et al*., 2021). The ability to conduct preliminary genetic assessments through simple smartphone photographs, enabled by omnipresent mobile devices that can recognize 3D faces with increasing precision (Togneri *et al*., 2019), could fundamentally alter the landscape of early detection and intervention for rare genetic diseases.

While the diagnostic capabilities of AI systems demonstrate remarkable promise, our analysis reveals that these same technologies introduce complex ethical, legal, and security challenges that must be carefully navigated (Ezeogu, *et al*.,2025). The high accuracy rates achieved by facial recognition algorithms, while medically beneficial, simultaneously raise profound privacy concerns regarding biometric data collection, storage, and potential misuse. The omnipresence of mobile devices capable of sophisticated facial recognition creates unprecedented opportunities for both beneficial healthcare applications and potentially harmful surveillance practices.

The forensic applications of AI-powered phenotyping present particularly nuanced implications. While these technologies could revolutionize missing persons investigations and aid in criminal identification (Wu *et al*., 2022), they also pose significant risks of discriminatory enforcement, wrongful identification, and erosion of civil liberties. The potential for AI-supported genetic applications to discriminate against minorities based on race, ethnicity, or health traits represents a critical ethical challenge that requires immediate attention from policymakers, technologists, and ethicists (Kovac *et al*., 2023). Various forensic applications can be significantly improved with AI applications, from morphometric analysis and AI behavioral analyses to age estimation in minors (Wan et al., 2022).

Our comprehensive threat assessment reveals that cybersecurity considerations are not merely technical add-ons but fundamental requirements for responsible AI implementation in healthcare. The identification of data poisoning and privacy leakage as critical threats underscores the vulnerability of AI systems to malicious actors who could compromise diagnostic accuracy or breach patient confidentiality. The sensitive nature of genomic data, combined with the potential for long-term harm from privacy breaches, demands robust protective measures that go beyond traditional healthcare cybersecurity approaches (Wan *et al*., 2022).

The emerging solutions identified in this review, including adversarial training, differential privacy, and homomorphic encryption, represent promising directions for securing AI healthcare systems. However, the fact that most mitigation strategies remain in development phases highlights the urgency of advancing cybersecurity research alongside AI diagnostic capabilities. The implementation of federated learning approaches offers promise for enabling collaborative AI development while maintaining data locality and privacy protection.

The regulatory landscape for AI in healthcare presents a complex web of challenges that extend far beyond traditional medical device regulation. The General Data Protection Regulation (GDPR) and similar privacy frameworks create significant implementation hurdles, particularly for facial recognition technologies that process sensitive biometric data (Thurzo et al., 2022). The cross-jurisdictional nature of modern healthcare delivery complicates compliance efforts, as AI systems must navigate varying legal requirements across different regions while maintaining consistent performance and safety standards.

The unclear allocation of liability for AI-driven diagnostic errors represents a fundamental challenge that requires urgent attention from legal scholars and policymakers. Questions of responsibility become particularly complex when AI systems are involved in diagnostic decisions, as traditional medical malpractice frameworks may not adequately address the unique characteristics of algorithmic decision-making. The need for human clinician oversight, while essential for safety (Rezende, 2020), creates additional complexity in determining appropriate levels of automation and human involvement in diagnostic processes.

The ethical implications of AI-driven genetic screening extend beyond traditional medical ethics to encompass fundamental questions of social justice, equity, and human rights. The potential for algorithmic bias to disproportionately affect minority populations represents a critical concern that could exacerbate existing health disparities if not properly addressed (Matthews *et al*., 2022). The complexity of informed consent for AI-specific applications requires new frameworks that help patients understand the implications of algorithmic analysis of their genetic and biometric data.

The question of data ownership in the context of AI-generated insights from patient data remains unresolved and represents a significant ethical and legal challenge. As AI systems derive new knowledge from patient data, questions arise about who owns these insights and how they should be used for future research and development. The potential for commercial exploitation of patient-derived AI insights raises concerns about fairness and benefit-sharing that require careful consideration. Any such study must be governed by ethical principles of autonomy, beneficence, non-maleficence, and justice.

The identified technical limitations, particularly dataset bias affecting rare disease populations, highlight fundamental challenges in AI development for healthcare applications. The small population sizes typical of rare diseases create unique challenges for machine learning approaches that typically require large, diverse datasets for optimal performance. This limitation necessitates innovative approaches to data augmentation, transfer learning, and collaborative data sharing that can enhance AI performance while maintaining patient privacy. The AI algorithm is only as good as its training dataset, and there is a risk, especially where rare disorders affect only small numbers of people (Coley *et al*., 2021).

The computational complexity required for genomic AI analysis represents both a technical challenge and an opportunity for advancing healthcare infrastructure. The need for substantial computational resources may limit accessibility in resource-constrained settings, potentially exacerbating health disparities. However, advances in cloud computing and edge AI technologies offer promising solutions for democratizing access to sophisticated AI diagnostic capabilities.

Successful implementation of AI-driven therapeutic molecule design and diagnostic systems requires a multifaceted approach that addresses technical, ethical, legal, and social considerations simultaneously. The identification of governance pillars including data quality standards, trust frameworks, standardization, and professional education provides a roadmap for responsible AI deployment in healthcare settings.

The emphasis on continuous monitoring and assessment of security risks and ethical implications reflects the dynamic nature of AI technology and the evolving threat landscape. Healthcare organizations must develop adaptive governance frameworks that can evolve with technological advances while maintaining essential safety and ethical standards. The need for collaboration between technologists, healthcare providers, policymakers, and ethicists underscore the interdisciplinary nature of successful AI implementation.

The potential for AI-driven diagnostic technologies to transform healthcare delivery extends beyond developed healthcare systems to resource-limited settings where these technologies could provide unprecedented access to specialized genetic expertise. The mobile accessibility of facial phenotyping applications could democratize genetic screening in regions where traditional genetic services are unavailable or prohibitively expensive (Hong *et al*., 2021). However, ensuring equitable access to these technologies requires careful attention to issues of digital divide, technological literacy, and healthcare infrastructure.

The cost-effectiveness of AI-driven screening approaches could enable population-level genetic screening programs that were previously economically unfeasible. Described artificial intelligence (AI) technologies could facilitate automated population screening for certain genetic traits or disorders without the need to obtain any biological sample from nation-states or even private companies (Bianchi *et al*., 2023). Such programs could facilitate early identification of genetic disorders, enabling timely intervention and potentially preventing serious health complications. However, the implementation of population-level screening programs raises additional ethical and privacy concerns that must be carefully addressed through comprehensive governance frameworks.

The potential uses of AI-powered phenotyping for law enforcement cannot be overstated (Kabata and Thaldar, 2023). This could revolutionize missing persons cases, helping investigators quickly match unidentified remains or photos of missing persons to facial scans in existing databases (Wu *et al*., 2022). Furthermore, facial recognition could aid in the identification of suspects from surveillance footage, providing valuable leads and potentially even allowing for identification based on genetic markers extracted via artificial intelligence (AI).

However, ethical considerations are paramount in this domain. Questions about consent, accuracy in suspect identification, and the potential for biases that could lead to wrongful convictions must be carefully navigated to ensure the responsible implementation of such powerful technologies (Brown, 2023). Law enforcement and intelligence agencies are, in some cases, exempt from privacy-protecting legislation and may obtain access to, process, and combine almost any type of personal data in the interest of national security. Without a doubt, AI applications in genetics can create extreme risks to privacy and anonymity (Kovac *et al*., 2023).

**Future Directions and Research Priorities**

The rapid evolution of AI technology in healthcare necessitates ongoing research across multiple domains. Priority areas include developing adversarial robust AI models that can resist malicious attacks, expanding training datasets to better represent rare disease populations, and creating real-time threat monitoring systems that can detect and respond to emerging cybersecurity challenges. The development of interoperability standards will be crucial for enabling secure data sharing across different healthcare systems and research institutions.

The harmonization of AI-specific healthcare regulations across jurisdictions represents a critical policy priority that could facilitate beneficial innovation while maintaining essential safety and ethical standards. The development of comprehensive ethical guidelines and patient rights protections will be essential for maintaining public trust and ensuring equitable access to AI-driven healthcare technologies. Looking at the GDPR perspective, consent, legal obligation, and public interest may be considered viable options for the selection of an appropriate legal basis (Thurzo et al., 2022).

**Conclusions**

AI-driven technologies have transitioned from theoretical potential to real-world clinical utility in the diagnosis and treatment of rare genetic diseases. Tools such as **Face2Gene** and **DeepGestalt** have demonstrated diagnostic accuracies exceeding 90%, outperforming traditional diagnostic approaches in recognizing rare syndromic features. In parallel, platforms like **AlphaFold** and **Atomwise** have significantly accelerated drug discovery and therapeutic molecule design, reducing time and cost while expanding possibilities for precision medicine.

Despite these advancements, widespread implementation demands more than technical excellence. It requires **secure, scalable infrastructures** supported by **robust cybersecurity frameworks,** including adversarial training, differential privacy, and homomorphic encryption, to protect highly sensitive genomic and clinical data. Equally important are **ethical safeguards** clear protocols for **informed consent, data ownership,** and **equitable access**, especially in underserved populations where healthcare disparities persist.

To achieve sustainable and responsible integration of AI into healthcare, **collaboration among clinicians, data scientists, policymakers, and ethicists** is essential. Regulatory alignment with frameworks such as the **GDPR** must guide deployment to ensure both innovation and accountability. Institutions must also invest in **capacity building**, training healthcare professionals to work alongside AI systems and interpret outputs critically.

Ultimately, the successful application of AI in rare disease research is not solely a technical challenge it is a societal one. The path forward must prioritize transparency, inclusiveness, and security to ensure that the benefits of AI reach all populations. By addressing practical, ethical, and legal concerns in tandem, AI can truly revolutionize personalized medicine and offer hope to the millions affected by rare genetic conditions.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

**Reference**

AlQahtani, S. M. Almutairi, D. S. BinAqeel, E. A. Almutairi, R. A. Al-Qahtani, R. D. Menezes, R.G. (2022). Honor Killings in the Eastern Mediterranean Region: *A Narrative Review. Healthcare* 2022, 11, 74.

Basch, C. H. Hillyer, G. C. Samuel, L. Datuowei, E. Cohn, B. (2022). Direct-to-consumer genetic testing in the news: A descriptive analysis. *J. Community Genet*. 2022, 14, 63–69.

Benchimol, E. I. Smeeth, L. Guttmann, A. (2015). RECORD Working Committee. The Reporting of studies Conducted using Observational Routinely-collected health Data (RECORD) statement. 2015; 12 (10): e1001885.

Bianchi, I. Oliva, G. Vitale, G. Bellugi, B. Bertana, G. Focardi, M. Grassi, S. Dalessandri, D. Pinchi, V. (2023). A Semi-Automatic Method on a Small Italian Sample for Estimating Sex Based on the Shape of the Crown of the Maxillary Posterior Teeth. *Healthcare,* 2023, 11, 845.

Brown, O. R. (2023). Marijuana: Forensics of Abuse, Medical Uses, Controversy, and AI. *Forensic Sci*. 2023, 3, 571–575.

Cameriere, R. Scendoni, R. Ferrante, L. Mirtella, D. Oncini, L. Cingolani, M. (2023). An Effective Model for Estimating Age in Unaccompanied Minors under the Italian Legal System. *Healthcare,* 2023, 11, 224.

Chorostowska-Wynimko, J. Wencker, M. Horváth, I. (2019). The importance of effective registries in pulmonary diseases and how to optimize their output. *Chron Respir Dis*. 2019; 16: 1479973119881777.

Cole, A. P. Friedlander, D. F. Trinh, Q. D. (2018).  Secondary data sources for health services research in urologic oncology. *Urology Oncology*.  2018; 36 (4): 165–73.

Coley, R. Y. Johnson, E. Simon, G. E. Cruz, M. Shortreed, S. M. (2021). Racial or Ethnic Disparities in the Performance of Prediction Models for Death by Suicide after Mental Health Visits. *JAMA Psychiatry*, 2021, 78, 726.

Cox-Brinkman, J. Vedder, A. Hollak, C. Richfield, L. Mehta, A. Orteu, K. Wijburg, F. Hammond, P. (2017). Three-dimensional face shape in Fabry disease. *Eur. J. Hum. Genet*., 15, 535–542.

Dudding-Byth, T. Baxter, A. Holliday, E. G. Hackett, A. O’Donnell, S. White, S.M. Attia, J. Brunner, H. De Vries, B. Koolen, D. (2017). Computer face-matching technology using two-dimensional photographs accurately matches the facial gestalt of unrelated individuals with the same syndromic form of intellectual disability. *BMC Biotechnology.* 2017, 17, 90.

Ezeogu, Favour Lewechi, Chidiebube Nelson Ozioko, Ihuoma Remita Uchenna, Innocent Junior Opara, and Salvation Ifechukwude Atalor. 2025. “Securing AI-Powered Healthcare Decision Support Systems: A Comprehensive Review of Attack Vectors and Defensive Strategies”. *Asian Journal of Advanced Research and Reports* 19 (6):1-11. <https://doi.org/10.9734/ajarr/2025/v19i61037>.

Feltelius, N. Gedeborg, R. Holm, L. (2017).  Utility of registries for post-marketing evaluation of medicines. A survey of Swedish health care quality registries from a regulatory perspective. *Ups J Med Sci.* 2017; 122 (2): 136–47.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International. Journal. Mark*. Res. 2017, 59, 703–705.

Gruschka, N. Mavroeidis, V. Vishi, K. Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5027–5033.

Gurovich, Y. Hanani, Y. Bar, O. Nadav, G. Fleischer, N. Gelbman, D. Basel-Salmon, L. Krawitz, P. M. Kamphausen, S. B. Zenker, M. (2019). Identifying facial phenotypes of genetic disorders using deep learning. *National. Medicine*. 2019, 25, 60–64.

Gurovich, Y., Hanani, Y., Bar, O., et al. (2019). Identifying facial phenotypes of genetic disorders using deep learning. *Nature Medicine*, 25(1), 60-64.

Haendel, M. Vasilevsky, N. Unni, D. Bologa, C. Harris, N. Rehm, H. Hamosh, A. Baynam, G. Groza, T. McMurry, J. (2020). How many rare diseases are there? *Nat. Rev. Drug Discov*. 2020, 19, 77–78.

Hong, D. Zheng, Y. Y. Xin, Y. Sun, L. Yang, H. Lin, M. Y. Liu, C. Li, B. N. Zhang, Z. W. Zhuang, J. (2021). Genetic syndromes screening by facial recognition technology: VGG-16 screening model construction and evaluation. *Orphanet J. Rare Dis*. 2021, 16, 344.

Iluno, C., and Nwaogwugwu, C. J., (2025). Applications of High-Performance Computing

(HPC) in Healthcare Diagnostics: A Systematic Review of AI-Driven Disease Prediction Models. *ISAR Journal of Medical and Pharmaceutical Sciences*, 3(3), 15-23.

Jaganathan, K., Kyriazopoulou Panagiotopoulou, S., McRae, J. F., et al. (2019). Predicting

splicing from primary sequence with deep learning. *Cell*, 176(3), 535-548

Kabata, F. Thaldar, D. (2023). The human genome as the common heritage of humanity. *Front. Genet.* 2023, 14, 1282515.

Kalokairinou, L. Howard, H. C. Slokenberga, S. Fisher, E. Flatscher-Thöni, M. Hartlev, M. van Hellemondt, R. Juškevičius, J. Kapelenska-Pregowska, J. Kováč, P. (2018). Legislation of direct-to-consumer genetic testing in Europe: A fragmented regulatory landscape. *J. Community Genet*. 2018, 9, 117–132.

Kapsner, L. A. Kampf, M. O. Seuchter, S. A. (2019).  Moving towards an EHR data quality framework: the MIRACUM approach. *Stud Health Technol Inform*, 2019; 267: 247–53.

Knight, A.W. (2016). Senior, T.P. The common problem of rare disease in general practice. *Med. J. Aust.,* 185, 82–83.

Kováč, P. Alexandra, B. Ivan, V. Lukáš, M. Michal, A. Martin, S. Thurzo, A. (2023). Phenotyping Genetic Diseases Through Artificial Intelligence Use of Large Datasets of Government-stored Facial Photographs: Concept, Legal Issues, and Challenges in the European Union. *Preprints*, 2023, 2023040344.

Latorre-Pellicer, A. Ascaso, Á. Trujillano, L. Gil-Salvador, M. Arnedo, M. Lucia-Campos, C. Antoñanzas-Pérez, R. Marcos-Alcalde, I. Parenti, I. Bueno-Lozano, G. (2020). Evaluating Face2Gene as a Tool to Identify Cornelia de Lange Syndrome by Facial Phenotypes. *International Journal. Molecular Science.* 2020, 21, 1042.

Leavy, M. B. Swenson, A. (2019). Data Sources In: Gliklich RE, Leavy MB, Dreyer NA, eds. Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User’s Guide, 3rd Edition, Addendum 2 [Internet]. Rockville, MD: Agency for Healthcare Research and Quality (US), 2019. Chapter 2.

Lumaka, A. Cosemans, N. Lulebo Mampasi, A. Mubungu, G. Mvuama, N. Lubala, T. Mbuyi-Musanzayi, S. Breckpot, J. Holvoet, M. De Ravel, T. (2017). Facial dysmorphism is influenced by ethnic background of the patient and of the evaluator. *Clinical Genetics*. 2017, 92, 166–171.

Matthews, H. De Jong, G. Maal, T. Claes, P. (2022). Static and Motion Facial Analysis for Craniofacial Assessment and Diagnosing Diseases. *Annu. Rev. Biomed. Data Sci*. 2022, 5, 19–42.

Mavrogiorgou, A. Kiourtis, A. Perakis, K. (2019).  Analyzing data and data sources towards a unified approach for ensuring end-to-end data and data sources quality in healthcare 4.0. *Computer Methods Programs Biomed*,  2019; 181: 104967.

Olczak, K. Pawlicka, H. Szymański, W. (2023). Root and canal morphology of the maxillary second premolars as indicated by cone beam computed tomography. *Aust. Endod. Journal.* 2023, 49, 92–103.

Porras, A. R. Rosenbaum, K. Tor-Diez, C. Summar, M. Linguraru, M. G. (2021). Development and evaluation of a machine learning-based point-of-care screening tool for genetic syndromes in children: A multinational retrospective study. *Lancet Digit. Health,* 2021, 3, e635–e643.

 Poplin, R., Chang, P. C., Alexander, D., et al. (2018). A universal SNP and small-indel variant caller using deep neural networks. *Nature Biotechnology*, 36(10), 983-987.

Rezende, I. N. (2020). Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective. *New J. Eur. Crim. Law*. 2020, 11, 375–389.

Richmond, S. Howe, L. J. Lewis, S. Stergiakouli, E. Zhurov, A. (2018). Facial Genetics: A Brief Overview. *Front. Genet*. 2018, 9, 462.

Roosenboom, J. Hens, G. Mattern, B. C. Shriver, M. D.; Claes, P. (2016). Exploring the Underlying Genetics of Craniofacial Morphology through Various Sources of Knowledge. *BioMed Res. Int*. 2016, 2016, 1–9.

Ruseckaite, R. Maharaj, A. D. Krysinska, K. (2019).  Developing a preliminary conceptual framework for guidelines on inclusion of patient reported-outcome measures (PROMs) in clinical quality registries. *Patient Relat Outcome Meas*. 2019; 10: 355–72.

Shabani, M. Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *Eur. J. Hum. Genet*. 2018, 26, 149–156.

Shade, J. Coon, H. Docherty, A. R. (2019). Ethical implications of using biobanks and population databases for genetic suicide research. *Am. J. Med. Genet*. Part B 2019, 180, 601–608.

Thurzo, A. Stanko, P. Urbanova, W. Lysy, J. Suchancova, B. Makovnik, M. Javorka, V. (2015) The WEB 2.0 Induced Paradigm Shift in the e-Learning and the Role of Crowdsourcing in Dental Education. *BratislLek. Listy,* 2015, 111, 168–175.

Thurzo, A. Strunga, M. Havlínová, R. Reháková, K. Urban, R. Surovková, J. Kurilová, V. (2022). Smartphone-Based Facial Scanning as a Viable Tool for Facially Driven Orthodontics? *Sensors*, 2022, 22, 7752.

Togneri R, Camponogara G, Soininen J-P. (2019). Foundations of Data Quality Assurance for IoT-based Smart Applications. In: Latin-American Conference on Communications (LATINCOM). *Salvador, Brazil: IEEE*; 2019: 1–6.

Viangteeravat, T. Anyanwu, M. N. Nagisetty, V. R. Kuscu, E. Sakauye, M. E. Wu, D. (2015).  Clinical data integration of distributed data sources using Health Level Seven (HL7) v3-RIM mapping. *J Clin Bioinform* ; 1: 32.

Wan, Z. Hazel, J. W. Clayton, E. W. Vorobeychik, Y. Kantarcioglu, M. Malin, B. A. (2022). Sociotechnical safeguards for genomic data privacy. *Nat. Rev. Genet*. 2022, 23, 429–445.

Wilson, D. (2017). Australian Biometrics and Global Surveillance. *Int. Crim. Justice Rev*. 2017, 17, 207–219.

Wu, X. Feng, X. Cao, X. Xu, X. Hu, D. López, M. B. Liu, L. (2022). Facial Kinship Verification: A Comprehensive Review and Outlook. *Int. J. Computer. Vis.* 2022, 130, 1494–1525.