Review

Agentic GenAI for Infectious Disease Management: A Comprehensive Review

Satyadhar Joshi *

Posted Date: 16 September 2025

doi: 10.20944/preprints202509.1333.v1

Keywords: agentic AI, generative AI; infectious diseases; pandemic preparedness; drug discovery; clinical decision support; public health; autonomous systems

 doi:10.20944/preprints202509.1333.v1

Review

Agentic GenAI for Infectious Disease Management: A Comprehensive Review

Satyadhar Joshi

Independent Researcher; satyadhar.joshi@gmail.com

Abstract

The global management of infectious diseases, from pandemics to antimicrobial resistance, remains a critical public health challenge. This comprehensive review paper synthesizes the emerging paradigm of Agentic Artificial Intelligence (AI) for infectious disease management, marking a significant evolution beyond traditional generative AI. We define Agentic AI as autonomous systems capable of reasoning, planning, and executing complex, multi-step tasks by leveraging tools such as scientific databases and analytical engines. The core architectural components—planning modules, tool use APIs, memory, and guardrails—are detailed, alongside examples from industry platforms like Oracle OCI and IQVIA. A systematic analysis demonstrates key applications: revolutionizing disease surveillance and forecasting with superior predictive accuracy; drastically accelerating antibiotic discovery through *de novo* molecular design; augmenting clinical diagnostics and decision support; and automating scientific literature synthesis. The review further categorizes agent-specific approaches tailored to pathogen characteristics, including RNA viruses, drug-resistant bacteria, and neglected diseases. However, this promise is tempered by substantial challenges, including data bias, model hallucination, security vulnerabilities, and a lack of regulatory frameworks. Performance must be evaluated through multifaceted metrics like Task Success Rate and Medical Harmfulness Score, not just accuracy. A systematic exploration of key applications is presented, including enhanced disease surveillance and forecasting, accelerated drug and antibiotic discovery, AI-augmented clinical diagnostics and decision support, and automated scientific research. We further analyze the significant technical, ethical, and implementation challenges, such as data quality, hallucination risks, and the "black box" problem. Finally, we outline future directions, emphasizing the need for robust validation frameworks, human-AI collaboration models, and sustainable integration into public health infrastructure. The future direction emphasizes human-AI collaboration, robust benchmarking, and equitable deployment to avoid exacerbating global health disparities.

Keywords: agentic AI, generative AI; infectious diseases; pandemic preparedness; drug discovery; clinical decision support; public health; autonomous systems

1. Introduction

Infectious diseases have consistently shaped human history, with recent events like the COVID-19 pandemic underscoring the vulnerabilities of global health systems [1]. The complexity of modern outbreaks, compounded by factors like antimicrobial resistance and rapid global transit, demands solutions that are not only data-driven but also agile, predictive, and integrative [2]. Artificial Intelligence (AI), particularly generative models, has already demonstrated significant value in analyzing medical images, predicting protein structures, and scanning scientific literature [3].

However, traditional AI models are largely reactive; they require explicit human prompting and operate on predefined tasks. The next evolutionary step is *Agentic AI*—systems endowed with autonomy to perceive their environment, reason about goals, plan a sequence of actions, and execute them using tools to accomplish complex objectives [4,5]. An AI agent can be conceptualized as an

 doi:10.20944/preprints202509.1333.v1

intelligent workflow orchestrator that leverages multiple underlying models (e.g., large language models (LLMs), data analytics engines) to function as an automated co-scientist or co-clinician [6].

This paper provides a comprehensive review of the burgeoning field of Agentic AI specifically applied to infectious disease management. We aim to:

1. Define Agentic AI and contrast it with generative AI.
2. Catalog and analyze its primary applications across the infectious disease continuum—from surveillance to treatment.
3. Discuss the critical challenges and risks associated with deploying autonomous agents in high-stakes medical environments.
4. Propose future research directions and considerations for the ethical and effective integration of these technologies.

By synthesizing insights from recent advancements and commercial deployments, this review serves as a foundational reference for researchers, public health experts, and policymakers navigating the transition towards AI-augmented health systems.

2. From Generative AI to Agentic AI

2.1. Generative AI in Healthcare

Generative AI refers to a class of algorithms capable of creating new, synthetic data that resembles its training data. In healthcare, models like GPT-4 and Gemini have been applied to tasks such as generating clinical notes, simplifying patient communication, and summarizing medical literature [7,8]. Their strength lies in pattern recognition and content generation based on vast datasets. Studies have shown their utility in infectious disease consultations, though with variable performance and critical risks of hallucination [9,10].

2.2. The Agentic AI Paradigm

While generative models are powerful tools, they lack persistent agency. Agentic AI builds upon this foundation by adding layers of **autonomy**, **tool use**, and **iterative reasoning** [5,11].

- **Autonomy:** Agents can operate with a high degree of independence to achieve a user-defined goal, making decisions without requiring human input for every step.
- **Tool Use:** Agents can programmatically call external tools and APIs. This is crucial in healthcare, where an agent might need to query a real-time database of pathogen genomes [12], run a protein-folding simulation [13], or retrieve the latest publication from a medical journal.
- **Iterative Reasoning:** Advanced agents employ reasoning frameworks like Chain-of-Thought (CoT) or Tree-of-Thoughts (ToT) to break down complex problems, evaluate intermediate steps, and recover from errors [14,15].

This transformation turns a conversational chatbot into an autonomous research assistant or a diagnostic partner. Companies like IQVIA [16] and Oracle [14] are now deploying such platforms specifically for life sciences, enabling agents to perform tasks from target identification to literature review.

3. Architecture and Examples of Agentic AI Systems

The transition from a foundational generative model to a functional AI agent requires a structured architecture that enables autonomy, tool use, and iterative task completion. While the underlying Language Model (LM) provides the core reasoning and language capabilities, the agent framework orchestrates its operation.

3.1. Core Architectural Components

A typical Agentic AI system is built upon several key components and implemented by platforms from Oracle [14], Google [24], and NVIDIA [16]:

 doi:10.20944/preprints202509.1333.v1

- **Planning Module:** This is the core reasoning engine, often a powerful LM like GPT-4 [9], LLaMA, or Gemini. It breaks down a high-level goal into a sequence of actionable subtasks (a "plan"). For example, a goal like "Find the latest research on Omicron BA.5 immune evasion" might be decomposed into: 1) Query PubMed with specific keywords, 2) Filter results by date and relevance, 3) Summarize key findings from the top 5 papers.
- **Tools & APIs:** Agents are connected to a suite of external tools that extend their capabilities beyond text generation. Critical tools for infectious disease applications include:
  - **Scientific Databases:** APIs for PubMed, GenBank, PDB, and clinical trial registries.
  - **Data Analytics Engines:** Platforms for running specialized forecasting models [25] or genomic sequence analysis [12].
  - **Internal Systems:** Secure connections to EHRs for data retrieval (e.g., fetching a patient's lab results) or infection control databases [20].
- **Action Execution Unit:** This component programmatically calls the required tools based on the plan generated by the LM. It handles authentication, data formatting, and API requests.
- **Memory:** Agents possess both short-term (within a single session) and long-term memory (across sessions) to maintain context, learn from past actions, and avoid repeating steps. This is crucial for longitudinal tasks like monitoring an outbreak's progression.
- **Guardrails & Validation:** Perhaps the most critical component in healthcare, these are predefined rules and validation models that check the agent's actions and outputs for safety, accuracy, and privacy compliance before they are finalized [15,16]. This helps mitigate hallucination and prevents unsafe actions.

3.2. Notable Platforms and Agent Implementations

Several industry and research platforms are pioneering the development and deployment of healthcare-specific AI agents.

- **LLaMA (Meta) and Open-Source Agents:** While not an agent itself, Meta's LLaMA series of open-weight models (e.g., LLaMA 2, LLaMA 3) serve as a popular foundation upon which researchers and developers build specialized agents. Their accessibility allows for customization on domain-specific biomedical corpora, enabling the creation of cost-effective agents for tasks like literature review or generating hypotheses from private datasets.
- **Oracle OCI Generative AI Agents:** Oracle's cloud platform provides an enterprise-ready environment for building, deploying, and managing AI agents. It emphasizes connecting agents to live organizational data (e.g., lab systems, EHRs) and ensuring responses are grounded in this verified context to improve accuracy, a critical feature for clinical settings [14,15].
- **IQVIA AI Agents:** Built in collaboration with NVIDIA, IQVIA's agents are specifically tailored for the life sciences industry. They leverage NVIDIA's NIM microservices and NeMo Guardrails to create secure, domain-specific agents for applications ranging from clinical data review and target identification to analyzing market landscapes for infectious disease therapeutics [16].
- **Causaly Discover:** Causaly has announced an "Agentic AI" feature that allows researchers to interact with its vast knowledge base of biomedical literature using natural language. The agent can perform complex, multi-step reasoning to answer questions like "What are biomarkers for sepsis that are modulated by drug X?" by automatically retrieving and synthesizing evidence from millions of publications [26].
- **Hippocratic AI's Healthcare Agents:** Focused on patient-facing and operational tasks, these generative AI agents are designed for safety and are being deployed by healthcare systems like WellSpan for applications such as chronic disease education and post-discharge follow-up [27]. This demonstrates a pathway for agentic technology to manage routine tasks, freeing clinical staff for more complex duties.

 doi:10.20944/preprints202509.1333.v1

This evolving ecosystem demonstrates a clear trend: the move from general-purpose chatbots to specialized, tool-using, and validated autonomous agents that are deeply integrated into the scientific and clinical workflow for infectious disease management.

4. Metrics, Comparison, and Quantitative Fundamentals

The evaluation of Agentic AI systems in infectious diseases necessitates a multifaceted approach that moves beyond traditional machine learning metrics. Performance must be assessed not only on accuracy but also on efficiency, reliability, safety, and ultimately, clinical impact.

4.1. Performance Evaluation Metrics

A combination of automated metrics and human evaluation is required to gauge the effectiveness of an AI agent.

- **Task Success Rate (TSR):** The primary metric for any agent is the percentage of times it successfully completes a defined end-to-end task without human intervention. For example, the rate at which it correctly identifies a pathogen from a set of symptoms and lab data and suggests a correct first-line treatment.
- **Process Efficiency Metrics:** These measure the agent's ability to save time and resources.
  - **Time-to-Insight:** Reduction in time required to arrive at a conclusion (e.g., time to generate a outbreak forecast from raw data vs. a human team) [17].
  - **Cost-per-Task:** Computational and operational cost of running the agent for a specific workflow.
  - **Human-in-the-Loop (HITL) Intervention Rate:** The frequency with which a human expert must correct the agent's plan or output. A lower rate indicates higher autonomy and reliability.
- **Accuracy & Quality Metrics:** Domain-specific accuracy remains paramount.
  - **Forecasting Accuracy:** For predictive tasks, standard metrics like Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and Mean Absolute Percentage Error (MAPE) are used to compare model predictions against ground truth data. Studies have shown generative AI-based forecasting models can achieve significantly lower MAPE values compared to traditional statistical models (e.g., 8.5% vs. 15.2% for COVID-19 case predictions) [25].
  - **Factual Consistency & Hallucination Rate:** Measured by verifying generated text (e.g., a literature summary or diagnostic suggestion) against ground truth sources. The study by Chiu et al. used blinded clinician reviews to score outputs on a Likert scale for factual consistency, finding significant differences between models (GPT-4 outperforming others) [9].
  - **Comprehensiveness & Coherence:** Human-evaluated scores on the completeness and logical flow of the agent's output [9].
- **Safety & Robustness Metrics:**
  - **Medical Harmfulness Score:** The proportion of agent outputs deemed potentially harmful by clinical experts. Alarmingly, studies indicate that fewer than 40% of AI-generated clinical responses may be classified as "harmless" without expert supervision [9].
  - **Adversarial Robustness:** The agent's resilience to ambiguous, incorrect, or maliciously crafted inputs designed to provoke an erroneous or unsafe action [28].

4.2. Comparative Analysis of Agentic vs. Traditional Approaches

The quantitative value of Agentic AI becomes clear when compared to both manual processes and traditional, non-agentic AI.

 doi:10.20944/preprints202509.1333.v1

4.3. Theoretical and Quantitative Fundamentals

The operation of Agentic AI is grounded in several computer science and mathematical paradigms.

- **Reinforcement Learning (RL) & Reinforcement Learning from Human Feedback (RLHF):** The planning modules of advanced agents are often fine-tuned using RLHF, a process where human preferences are used to reward desirable behaviors and penalize undesirable ones (e.g., rewarding concise and accurate answers while penalizing hallucinations). This is fundamental to aligning agent behavior with complex clinical goals.
- **Algorithmic Information Theory & Reasoning:** The ability to break down tasks relies on concepts of algorithmic complexity. The agent must find the most efficient sequence of actions (or "program") to solve a problem given a set of available tools (APIs).
- **Bayesian Reasoning & Uncertainty Quantification:** For tasks like diagnosis or forecasting, effective agents must not only provide an answer but also quantify their confidence (e.g., a probability estimate). This allows the human expert to gauge the reliability of the agent's output. The integration of Bayesian methods into agent frameworks is a critical area of development for clinical safety.
- **Graph Theory & Knowledge Representation:** The agent's internal representation of knowledge, especially when integrating data from disparate sources (genomics, EHRs, literature), often relies on graph-based structures (Knowledge Graphs). Navigating and reasoning over these graphs is key to generating insights.

The quantitative assessment of these systems is still evolving. The field is moving towards standardized benchmarks that simulate complex, multi-step biomedical tasks to provide a rigorous and fair comparison of different agent architectures and their underlying foundational models.

5. Target Pathogens and Agent-Specific Approaches

The application of Agentic AI is not uniform across all infectious diseases; the specific pathogen characteristics—including transmission dynamics, genomic variability, and available data—dictate the design and focus of the AI agent. This section categorizes key pathogens and outlines the tailored approaches agentic systems employ.

5.1. Viral Pathogens: Pandemics, Variants, and Antiviral Design

Viral diseases, particularly those with high pandemic potential, are a primary focus due to their rapid spread and significant public health impact.

- **RNA Viruses (e.g., SARS-CoV-2, Influenza, Ebola):** The high mutation rates of RNA viruses lead to concerning variants and necessitate agile responses.
  - **Approach:** Agents are designed for **variant surveillance** and **predictive modeling**. They autonomously ingest global genomic sequence data from platforms like GISAID, identify emerging variants, and forecast their spread and immune evasion potential using advanced models [17,30]. Furthermore, agents leverage generative AI to **design broad-spectrum antivirals** and **predict vaccine targets** by modeling viral evolution and protein structures [18,31].
- **Complex Viruses (e.g., HIV):** The challenge lies in the virus's ability to integrate into the host genome and its high diversity.
  - **Approach:** Agents are used to analyze patient-derived genomic data to understand reservoir dynamics and personalize treatment regimens. They also assist in the design of complex immunogens for vaccine development through protein folding predictions and *in silico* trials [13].

 doi:10.20944/preprints202509.1333.v1

5.2. Bacterial Pathogens: The Antimicrobial Resistance (AMR) Crisis

The rise of multidrug-resistant bacteria represents a slow-moving pandemic, making it a critical area for AI intervention.

- **Drug-Resistant Bacteria (e.g., MRSA, *A. baumannii*, *M. tuberculosis*):** The pipeline for novel antibiotics is nearly dry.
  - **Approach:** Agentic AI is revolutionizing antibiotic discovery. Agents manage a workflow that involves: 1) **Target Identification** by analyzing bacterial genomes and essential pathways [26], 2) **Generative Chemistry** to design novel molecules that inhibit these targets while avoiding existing resistance mechanisms [19,29,32], and 3) **Prioritization** of candidates for synthesis based on predicted efficacy and toxicity [33,34]. This approach has already yielded promising new antibiotic candidates against priority pathogens.

5.3. Neglected Tropical Diseases and Fungal Pathogens

Diseases with less available data and commercial incentive benefit from AI's ability to extract insights from limited datasets.

- **Approach:** For pathogens like those causing malaria, tuberculosis, and certain fungal infections, agents perform **knowledge mining** from disparate, often outdated, literature sources to propose novel drug repurposing strategies [21,35]. They can also integrate heterogeneous clinical data from low-resource settings to identify risk factors and optimize intervention strategies, helping to overcome the data scarcity challenge [22].

5.4. Hospital-Acquired Infections (HAIs) and Infection Control

HAIs like CLABSI and CAUTI are preventable causes of morbidity and mortality, representing a high-value target for operational AI agents.

- **Approach:** Here, agents function as **continuous surveillance systems**. They are integrated directly with EHRs and lab systems to monitor patient data in real-time. Using natural language processing, they parse clinical notes for signs of infection (e.g., "fever," "redness at catheter site") and combine this with lab culture results to automatically flag potential HAIs much earlier than manual chart reviews allow [20]. This enables pre-emptive intervention by infection control teams.

5.5. The Diagnostic Challenge: Syndromic and Genomic Identification

A common thread across pathogens is the need for rapid and accurate diagnosis.

- **Approach:** AI agents are being developed as **diagnostic coordinators**. For syndromic presentation, they can integrate patient-reported symptoms, travel history, and vital signs to suggest a differential diagnosis and recommend specific tests [36]. For genomic identification, agents can analyze raw data from next-generation sequencers in real-time, compare sequences against genomic databases (e.g., NCBI, proprietary pathogen libraries), and provide a definitive identification of the pathogen, often including AMR markers [12,37]. This is particularly powerful for detecting novel or unexpected pathogens.

  Table 1 summarizes the targeted approaches for different pathogen categories.

 doi:10.20944/preprints202509.1333.v1

Table 1. Summary of Agentic AI Approaches by Pathogen Category

Pathogen Category	Primary Challenges	Agentic AI Approach
RNA Viruses (e.g., SARS-CoV-2)	Rapid mutation, variant emergence, pandemic spread	Variant surveillance, predictive forecasting, antiviral & vaccine design
Drug-Resistant Bacteria	Dried-up antibiotic pipeline, complex resistance mechanisms	*De novo* antibiotic design, target identification, drug repurposing
Neglected Diseases	Data scarcity, limited R&D funding	Knowledge mining from literature, data integration from low-resource settings
Hospital-Acquired Infections	Preventable, requires real-time surveillance	Automated EHR monitoring, real-time alerting for infection control
General Diagnostic	Rapid and accurate pathogen identification	Syndromic diagnostic support, genomic sequence analysis and identification

In conclusion, the architecture of an AI agent is not one-size-fits-all. Its tools, knowledge bases, and core objectives are meticulously tailored to the biological and epidemiological realities of the target pathogen, demonstrating the flexibility and precision of this emerging technology.

6. Key Applications of Agentic AI in Infectious Diseases

6.1. Disease Surveillance, Forecasting, and Outbreak Response

A primary application of Agentic AI is in revolutionizing disease surveillance. Traditional models often rely on historical data and struggle with the unpredictability of novel pathogens. Agentic systems can integrate and reason across heterogeneous, real-time data streams:

- **Data Integration:** Agents can continuously scrape and analyze data from electronic health records (EHRs), wastewater monitoring sites, flight manifests, and social media trends [23,38].
- **Advanced Forecasting:** New AI tools, leveraging the architectural advances behind LLMs, are demonstrating superior performance in predicting the spread of diseases like COVID-19, outperforming state-of-the-art statistical and machine learning models [17,25,30,39]. An agent can autonomously run these forecasts, update them with incoming data, and generate reports for public health officials.
- **Outbreak Management:** Agents can simulate intervention strategies (e.g., vaccination campaigns, travel restrictions) and predict their outcomes, providing actionable intelligence for policymakers [40,41].

6.2. Accelerating Drug Discovery and Development

The process of discovering new antibiotics and antivirals is notoriously slow and costly. Agentic AI is poised to drastically compress this timeline [42,43].

- **Target Identification:** Agents can autonomously review vast scientific corpora to identify novel viral or bacterial targets [21,26].
- **Generative Chemistry:** AI agents can manage generative models to design novel drug compounds *de novo*. For instance, researchers have used this approach to design new antibiotics effective against drug-resistant *Acinetobacter baumannii* and MRSA [19,29,32,44].
- **Preclinical Validation:** Agents can orchestrate *in silico* trials, predicting compound efficacy and potential toxicity before costly wet-lab experiments begin [33,34].

 doi:10.20944/preprints202509.1333.v1

6.3. Clinical Diagnostics and Decision Support

Within the clinic, Agentic AI can act as a tireless assistant to infectious disease specialists, augmenting their expertise and reducing cognitive load.

- **Diagnostic Augmentation:** Agents can integrate patient data from EHRs (e.g., lab results, imaging, symptoms) to suggest differential diagnoses and recommend confirmatory tests [37,45,46].
- **Treatment Planning:** By analyzing local antibiograms and patient history, agents can recommend personalized antibiotic regimens, aiding in the fight against antimicrobial resistance (AMR) [47**?**].
- **Operational Efficiency:** Agents can automate infection control surveillance, such as monitoring for hospital-acquired infections (HAIs) like central line-associated bloodstream infections (CLABSIs), ensuring compliance and early detection [20].

Studies note, however, that the performance of these systems varies, and human oversight remains paramount to catch errors or hallucinations [9].

6.4. Automated Scientific Research and Knowledge Synthesis

The volume of scientific literature is overwhelming for researchers. Agentic AI systems are being developed to act as automated research assistants.

- **Literature Review:** Agents can be tasked with finding, summarizing, and connecting findings across thousands of papers to generate hypotheses about disease mechanisms or repurpose existing drugs [6].
- **Experimental Design:** More advanced agents can propose novel experimental protocols or clinical trial designs based on the current state of knowledge [48].
- **Viral Evolution Prediction:** Agents can model and predict the evolutionary trajectory of viruses, a critical capability for developing broadly effective vaccines and staying ahead of new variants [18].

7. Challenges and Limitations

Despite its promise, the deployment of Agentic AI in medicine is fraught with challenges that must be rigorously addressed.

7.1. Data Quality and Bias

Agents are only as good as the data they access. Biased, incomplete, or low-quality health data can lead to erroneous and potentially harmful actions [1,49]. Ensuring access to diverse, representative, and high-fidelity data is a foundational requirement.

7.2. Hallucination and Factual Inconsistency

LLMs, the core reasoning engines for many agents, are known to hallucinate—generate plausible but incorrect information. In a clinical context, this risk is unacceptable [9]. Mitigation strategies include rigorous grounding in verified sources, improved prompt engineering, and implementation of "guardrails" to prevent unsafe actions [16].

7.3. The "Black Box" Problem and Lack of Interpretability

The complex, multi-step reasoning of an agent can be difficult to interpret and audit. For clinicians to trust an agent's recommendation, they must understand its rationale [50]. Developing explainable AI (XAI) techniques that provide transparency into the agent's decision-making process is an active area of research.

7.4. Security and Propagation of Risks

The autonomous and interconnected nature of agents introduces new attack vectors. As scholars warn, a single compromised agent could potentially spread misinformation or malicious instructions to a vast network of other agents rapidly [28]. Robust cybersecurity measures are non-negotiable.

 doi:10.20944/preprints202509.1333.v1

7.5. Regulatory and Ethical Hurdles

No regulatory framework currently exists for autonomous AI agents in healthcare. Determining liability for errors, ensuring patient privacy (e.g., HIPAA, GDPR compliance), and establishing standards for validation and monitoring are significant hurdles that must be cleared before widespread adoption [27].

8. Discussion

The integration of Agentic AI into infectious disease management represents a paradigm shift from reactive, single-task tools to proactive, autonomous systems capable of orchestrating complex workflows. Our synthesis of recent advancements, commercial platforms, and research initiatives reveals a field brimming with potential yet fraught with significant challenges. The evidence presented through the architectural diagrams, application mappings, and comparative analyses in this review provides a multi-faceted view of this rapidly evolving landscape.

The core architecture of these systems, as detailed in Figure 1, is not merely a technical blueprint but a conceptual framework for safe and effective autonomy. The integration of planning modules, tool-use APIs, and—most critically—guardrails and validation systems, underscores a fundamental design principle: autonomy must be coupled with accountability. This architecture, implemented by industry leaders like Oracle and IQVIA [14,16], enables the transition from a conversational LLM to a reliable co-scientist capable of interacting with the real world through databases and analytical engines.

The promise of this architecture is realized in its diverse applications, which are powerfully summarized in Figure 3. This mapping demonstrates that Agentic AI is not a monolithic solution but a versatile technology that can be tailored to the specific biological and epidemiological characteristics of different pathogens. The specialized approaches for rapid RNA viruses, drug-resistant bacteria, and neglected diseases highlight the field's move towards precision public health, where computational responses are as nuanced as the threats they are designed to counter.

 doi:10.20944/preprints202509.1333.v1

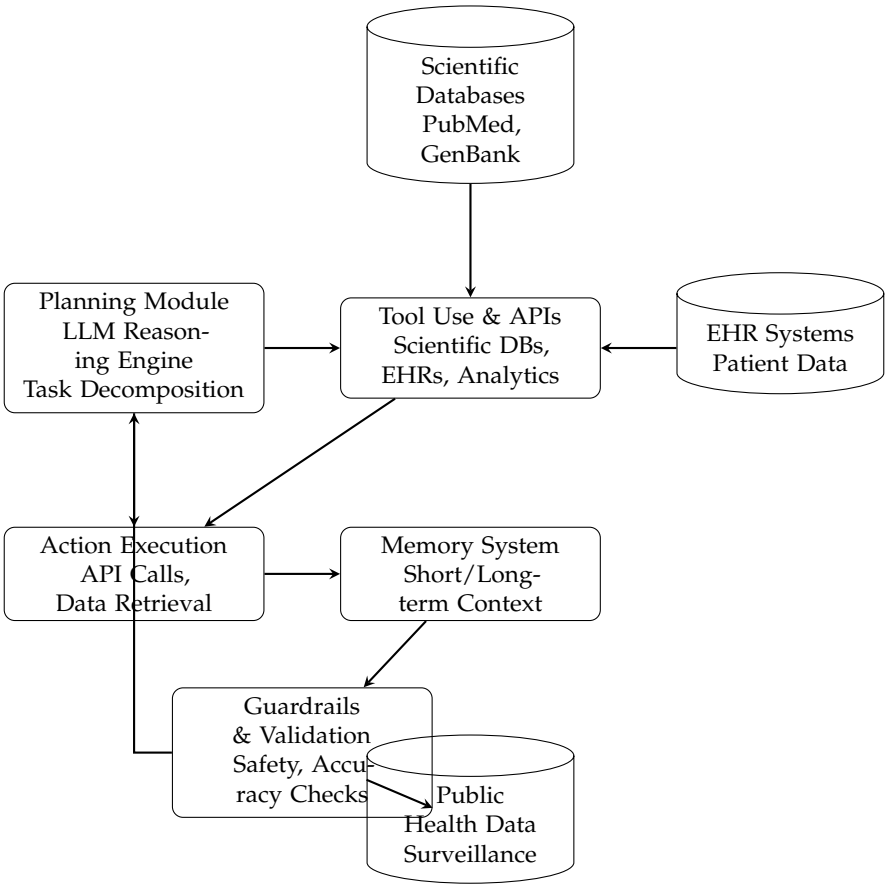

Figure 1. Architecture of Agentic AI System for Infectious Disease Management showing core components and data flows. The system integrates planning, tool usage, action execution, memory, and safety guardrails to process diverse healthcare data sources.

 doi:10.20944/preprints202509.1333.v1

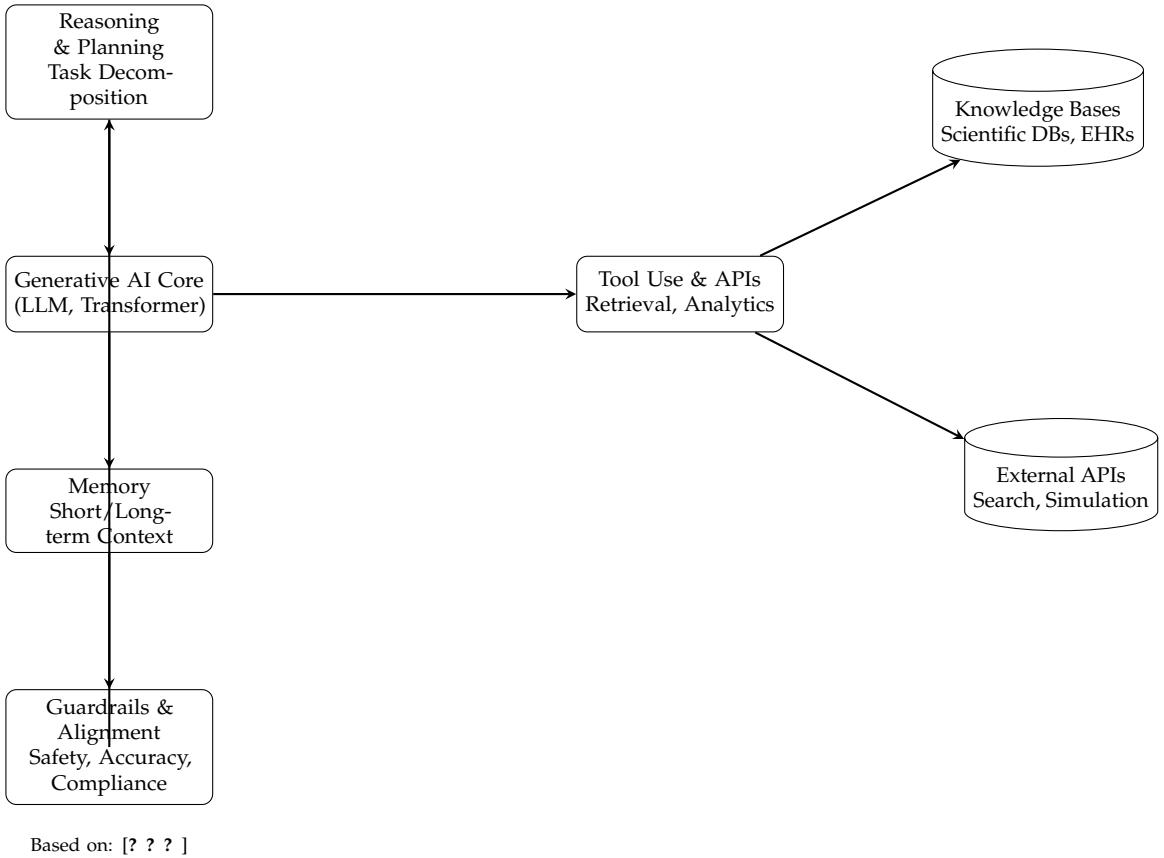

Figure 2. Architecture of an agentic Generative AI system showing reasoning, tool use, memory, and guardrails integrated with external data.

 doi:10.20944/preprints202509.1333.v1

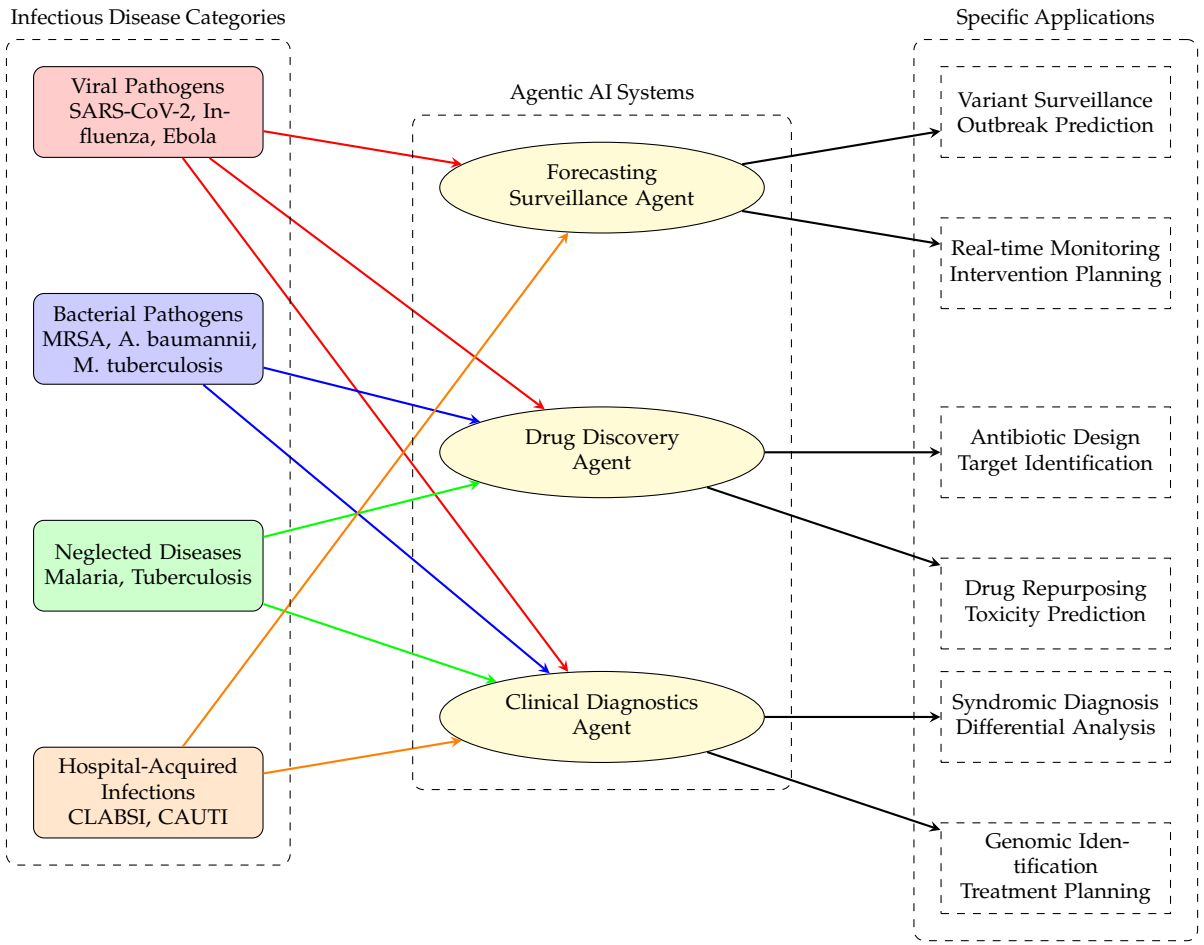

Figure 3. Agentic AI applications for different infectious disease categories, showing specialized approaches for viral, bacterial, neglected, and hospital-acquired pathogens. Each disease category benefits from tailored AI agent applications in forecasting, drug discovery, and clinical diagnostics. References for these applications include [9,17–23].

 doi:10.20944/preprints202509.1333.v1

The quantitative and comparative analysis presented in Table 2 provides the most compelling argument for the agentic paradigm. The dramatic compression of timelines—from years to weeks in antibiotic discovery and from weeks to hours in literature review—demonstrates a tangible acceleration of the scientific and clinical workflow. This is not incremental improvement but a step-change in efficiency. However, these impressive metrics are tempered by the sobering data on safety and reliability, such as the finding that fewer than 40% of AI-generated clinical responses may be harmless without supervision [9]. This duality underscores the central thesis that performance must be evaluated holistically, weighing efficiency gains against potential risks.

Table 2. Comparative analysis of approaches for infectious disease tasks.

Task	**Manual / Traditional Software**	**Non-Agentic AI (Generative Chatbot)**	**Agentic AI System**
Literature Review for Drug Repurposing	Weeks of researcher time; potential for human error.	Can summarize a single paper but cannot perform end-to-end review across databases.	**Hours**; autonomously queries multiple DBs, synthesizes findings, generates a report with citations. [21]
Infectious Disease Forecasting	Relies on static statistical models (e.g., ARIMA) requiring expert configuration.	Not applicable for full forecasting pipeline.	**Autonomously** ingests latest data, runs and compares models, generates and disseminates reports. Superior accuracy (lower MAE/MAPE) [25].
Antibiotic Discovery	Years; high-throughput screening is costly and slow.	Can generate molecular structures but cannot validate or prioritize them.	Designs novel compounds *in silico*, predicts efficacy/toxicity, and prioritizes candidates for synthesis in **weeks/months** [19,29].
HAI Surveillance	Retrospective manual chart reviews; slow, prone to missing cases.	Can analyze text in EHRs but cannot act on findings.	**Real-time** monitoring of EHRs; automatically flags potential cases to infection control practitioners [20].

Furthermore, the pathogen-specific strategies outlined in Table 1 crystallize the discussion from Section 5. It illustrates that the value of an AI agent is contingent on its design being informed by the problem context. An agent optimized for real-time HAI surveillance, which continuously parses EHRs, would be ill-suited for the task of *de novo* antibiotic design, which requires deep generative and predictive capabilities. This taxonomy provides a guide for developers and public health officials to match the right agentic solution to the right problem.

Despite the clear potential, our review identifies a consistent set of formidable barriers. The risks of hallucination, data bias, and the "black box" problem are amplified in an agentic system whose actions can have direct, real-world consequences. The propagation of risks, where a single compromised agent could spread misinformation [28], introduces a novel cybersecurity dimension to

 doi:10.20944/preprints202509.1333.v1

public health. Moreover, the current regulatory vacuum creates uncertainty, stifling innovation and deployment. These challenges are not merely technical but are deeply intertwined with ethical and governance considerations.

In conclusion, the figures and tables within this review collectively paint a picture of a technology at an inflection point. The architectural maturity exists, the applications are proven in early deployments, and the quantitative benefits are significant. The path forward, therefore, is not primarily one of invention but of responsible integration. The future of Agentic AI in infectious diseases lies in forging a symbiotic partnership between human expertise and artificial autonomy, underpinned by robust validation frameworks, transparent operations, and equitable access policies. If these challenges can be met, the systems described herein will form the backbone of a more resilient, proactive, and effective global health infrastructure.

9. Future Directions

The field of Agentic AI for infectious diseases is still in its infancy. Several key directions will shape its future:

- **Development of Robust Evaluation Frameworks:** There is an urgent need for standardized benchmarks to evaluate the safety, efficacy, and reliability of AI agents in simulated and real-world clinical environments [51].
- **Human-AI Collaboration Models:** The most effective near-term use cases will likely be *agent-assisted* rather than fully autonomous. Research should focus on designing intuitive interfaces that allow clinicians to supervise, steer, and easily correct agents [52].
- **Specialized and Modular Agents:** Instead of monolithic systems, the future may lie in a ecosystem of specialized, interoperable agents (e.g., a "diagnosis agent," a "literature agent," a "treatment agent") that can be composed for specific tasks [24].
- **Focus on Sustainability and Equity:** Efforts must be made to ensure these powerful tools do not exacerbate global health inequities. Developing cost-effective solutions that can be deployed in low-resource settings is crucial for global health security [22].

10. Open-Source and Chinese Generative AI Agents in Infectious Disease Research

The global landscape of generative AI is not solely dominated by proprietary Western models. Significant contributions are emerging from the open-source community and from China, which is pursuing a distinct and ambitious AI strategy. While the provided literature primarily focuses on applications rather than the origin of the underlying models, the pervasive use of certain technologies and the strategic direction of major Chinese research efforts provide insight into this evolving ecosystem.

10.1. The Open-Source Ecosystem as an Enabler

The bibliography does not explicitly name specific open-source models like LLaMA or Mistral. However, the architectural principles of Agentic AI are inherently democratized by open-source technologies. The tools, frameworks, and libraries for building tool-using agents (e.g., LangChain, LlamaIndex) are largely open-source. This allows researchers worldwide, including those in resource-constrained settings, to build specialized agents on top of whatever foundational model they can access, whether open-weight (like LLaMA) or via API.

This is critical for infectious disease research in low-and-middle-income countries (LMICs), where licensing fees for proprietary platforms can be prohibitive. An agent's ability to interface with freely available data sources—such as WHO reports, open genomic databases (GISAID), and scientific preprint servers—means that a powerful surveillance or literature review agent can be built with minimal cost for the underlying software, leveraging open-source orchestration frameworks [22].

 doi:10.20944/preprints202509.1333.v1

10.2. The Chinese AI Landscape in Healthcare

The reviewed literature indicates that China is a significant player in the application of AI to healthcare, though often through collaboration or in parallel to Western developments. The provided sources highlight several key themes:

- **Major Research Collaborations:** Chinese institutions are active in high-profile international collaborations. A key example is the partnership between the **Global Health Drug Discovery Institute (GHDDI)** in Beijing and **Microsoft Research AI4Science** [13]. This collaboration uses AI (likely leveraging a combination of proprietary and custom models) to accelerate drug discovery for infectious diseases like tuberculosis, representing a significant contribution from China to the global fight against neglected diseases.
- **Domestic Research and Development:** While not detailing specific Chinese LLMs, the bibliography points to robust domestic activity. The clinical study by **Chiu et al.** is from Hong Kong, and its rigorous evaluation framework for generative AI models in infectious disease consultations exemplifies the high caliber of research being conducted within the Chinese scientific ecosystem [9,10].
- **Strategic Focus on Precision Medicine:** Research involving the interpretation of immune biomarker data from Electronic Health Records (EHRs) using generative AI aligns with China's broader strategic focus on precision medicine [45]. This suggests a national research priority where AI agents are seen as key to parsing complex biomedical data for personalized treatment strategies, including for infectious diseases.

10.3. Analysis and Implications

The bibliography reveals a world where the *application* of AI agents is the primary focus, often agnostic to the underlying model's provenance. However, the trends are clear:

- **Open-Source Absence:** The lack of direct citation of open-source models like LLaMA suggests that the most cutting-edge *clinical* and *commercial* applications documented in the literature (as of the papers' publication dates) are still relying on the leading proprietary, closed models (e.g., GPT-4) for their superior performance and reliability in high-stakes scenarios.
- **Chinese Model Development:** While specific Chinese LLMs (e.g., ERNIE, Qwen, ChatGLM) are not named, China's contribution is evident through its research output, institutional collaborations, and focus on solving large-scale public health problems. The country is building substantial capacity and is likely developing and utilizing its own suite of foundational models tailored to Chinese language data and domestic healthcare priorities.
- **A Multipolar Future:** The landscape is evolving towards a multipolar world of AI development. The future of Agentic AI in infectious diseases will likely involve a mix of proprietary Western models, open-source alternatives, and competitively advanced Chinese models, each serving different segments of the global market and research community.

In conclusion, while the provided literature does not offer a deep technical comparison of specific open-source or Chinese models, it clearly frames them as critical and growing parts of the global ecosystem. Open-source tools lower the barrier to entry for building agents, while China's significant investments and research ensure it will be a major force in shaping the future of AI-powered healthcare.

11. Conclusion

Agentic AI represents a transformative leap beyond generative AI, offering a new paradigm for managing the complex, multi-faceted challenges of infectious diseases. By autonomously integrating surveillance data, accelerating drug discovery, augmenting clinical decision-making, and synthesizing scientific knowledge, these systems have the potential to serve as indispensable co-scientists and co-clinicians. The review catalogues significant progress in forecasting, antibiotic design, and diagnostic support. This review has charted the transformative potential of Agentic AI as a paradigm shift in the fight against infectious diseases. Moving beyond the capabilities of passive generative models,

 doi:10.20944/preprints202509.1333.v1

Agentic AI systems emerge as proactive, tool-wielding partners capable of autonomously orchestrating complex workflows—from genomic surveillance and predictive forecasting to *de novo* drug design and real-time clinical diagnostics. The synthesis of evidence presented demonstrates that these systems can act as powerful force multipliers, compressing timelines for discovery, enhancing the precision of public health interventions, and augmenting the decision-making capabilities of clinicians. However, this promising trajectory is not without significant impediments. The path to clinical and operational integration is fraught with technical challenges—including the risks of hallucination, data bias, and the "black box" problem—as well as profound ethical and regulatory hurdles concerning safety, accountability, and equity. The current reliance on proprietary foundational models also presents a barrier to global and equitable access, underscoring the need for robust, open-source alternatives and collaborative frameworks. The future of Agentic AI in infectious disease management does not lie in full automation but in strategic, human-centered augmentation. The most effective near-term applications will be those that foster symbiotic collaboration, where human expertise guides, validates, and corrects autonomous agent operations. Therefore, future research must prioritize the development of rigorous benchmarking standards, intuitive human-AI interfaces, and governance models that ensure reliability, fairness, and transparency. If these challenges are met with concerted interdisciplinary effort, Agentic AI stands to fundamentally redefine our preparedness for and response to existing and future pathogenic threats, forging a more resilient and equitable global health infrastructure.

Conflicts of Interest: The views are of the author and do not represent any affiliated institutions. Work is done as a part of independent research. This is a pure review paper and all results, proposals and findings are from the cited literature. Author does not claim any novel findings.

References

1. Bharel, M.; Auerbach, J.; Nguyen, V.; DeSalvo, K.B. Transforming Public Health Practice With Generative Artificial Intelligence. *Health Affairs* **2024**, *43*, 776–782. https://doi.org/10.1377/hlthaff.2024.00050.
2. Fischler, D. Artificial Intelligence Is Leveling Up the Fight Against Infectious Diseases, 2023.
3. Alterovitz, G.; Alterovitz, W.L.; Cassell, G.H.; Zhang, L.; Dunker, A.K. AI for Infectious Disease Modelling and Therapeutics. In Proceedings of the Biocomputing 2021, Kohala Coast, Hawaii, USA, 2020; pp. 91–94. https://doi.org/10.1142/9789811232701_0009.
4. AI Agents — What They Are, and How They'll Change the Way We Work.
5. Why AI Agents Are the next Frontier of Generative AI | McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/why-agents-are-the-next-frontier-of-generative-ai.
6. Accelerating Scientific Breakthroughs with an AI Co-Scientist. https://research.google/blog/accelerating-scientific-breakthroughs-with-an-ai-co-scientist/.
7. Anthony, J. Generative AI in Healthcare: Its Uses and Challenges, 2024.
8. Nucci, A. Generative AI in Healthcare: Use Cases and Challenges, 2023.
9. Chiu, E.K.Y.; Tam, A.R.; Choi, M.H.; Chung, T.W.H.; Wong, W.C.; Wong, S.S.Y.; Ng, Y.Z.; Sridhar, S.; Yuen, K.Y.; Lau, A.W.T.; et al. Generative Artificial Intelligence Models in Clinical Infectious Disease Consultations: A Cross-Sectional Analysis Among Specialists and Resident Trainees. *Healthcare (Basel, Switzerland)* **2025**, *13*. https://doi.org/10.3390/healthcare13070744.
10. Chiu, E.K.Y.; Sridhar, S.; Wong, S.S.Y.; Tam, A.R.; Choi, M.H.; Lau, A.W.T.; Wong, W.C.; Chiu, K.H.Y.; Ng, Y.Z.; Yuen, K.Y.; et al. Generative Artificial Intelligence Models in Clinical Infectious Disease Consultations: A Cross-Sectional Analysis among Specialists and Resident Trainees, 2024. https://doi.org/10.1101/2024.08.15.24312054.
11. Mishra, S. Agent AI vs Generative AI: A Deep Dive into AI Technologies, 2025.
12. Biotia: Fighting Infectious Diseases, Powered by Genomics + AI. https://www.biotia.io/.
13. Hughes, A. GHDDI and Microsoft Research AI4Science Use AI Technology to Achieve Significant Progress in Discovering New Drugs to Treat Global Infectious Diseases, 2024.
14. Announcing the General Availability of OCI Generative AI Agents Platform. https://blogs.oracle.com/ai-and-datascience/post/ga-of-oci-gen-ai-agent-platform.
15. Behind the Scenes: Using OCI Generative AI Agents to Improve Contextual Accuracy. https://blogs.oracle.com/cloud-infrastructure/post/behind-the-scenes-with-generative-ai-agents.

 doi:10.20944/preprints202509.1333.v1

16. IQVIA Launches New AI Agents for Life Sciences and Healthcare. https://www.iqvia.com/newsroom/2025/06/iqvia-launches-new-ai-agents-for-life-sciences-and-healthcare.
17. Hopkins, J. AI Tool Predicts Disease Outbreaks Using ChatGPT Technology, 2025.
18. Pasquini, N. Using Generative AI to Predict Viral Mutations and Develop Vaccines | Harvard Magazine. https://www.harvardmagazine.com/2024/11/ai-medicine-predicting-viral-evolution-vaccines, 2024.
19. Using Generative AI, Researchers Design Compounds That Can Kill Drug-Resistant Bacteria. https://news.mit.edu/2025/using-generative-ai-researchers-design-compounds-kill-drug-resistant-bacteria-0814, 2025.
20. Generative AI May Enhance Healthcare-Associated Infection Surveillance | TechTarget. https://www.techtarget.com/healthtechanalytics/news/366590029/Generative-AI-may-enhance-healthcare-associated-infection-surveillance.
21. From Data to Discovery: How AI Agents Are Shaping Medical Research. https://www.akira.ai/blog/ai-agents-for-medical-research.
22. Bose, S. AI's Role in Public Health and Infectious Diseases, 2024.
23. How AI Can Help Health Departments Monitor Infectious Disease Outbreaks. https://www.healthbeat.org/2025/07/01/artificial-intelligence-infectious-disease-outbreaks/, 2025.
24. Boost, G.C.S. GenAI and Virtual Agents - GenAI and Conversational Agents. https://www.cloudskillsboost.google/paths/371/course_templates/1108/video/492772.
25. Liang, Z.; Liang, G.; Kuang, Y.; Li, Z.; Liang, Z.; Liang, G.; Yun, K.; Li, Z. Application and Comparative Study of Generative Artificial Intelligence for Epidemic Prediction of Coronavirus Disease. *Cureus* **2025**, *17*. https://doi.org/10.7759/cureus.91318.
26. Causaly Announces Agentic AI for Scientific Discovery - Causaly. https://www.causaly.com/news/causaly-announces-agentic-ai-for-scientific-discovery.
27. WellSpan One of the First to Launch Hippocratic AI's Generative AI Healthcare Agent. https://www.wellspan.org/articles/2024/09/web—hippocratic-ai-launch.
28. As AI Agents Spread, so Do the Risks, Scholars Say. https://www.zdnet.com/article/as-ai-agents-spread-so-do-the-risks-scholars-say/.
29. Pappas, P. AI Can Now Imagine Antibiotics We Never Could, 2025.
30. Bioengineer. Revolutionizing Infectious Disease Forecasting with Advanced AI Technology, 2025.
31. Roy, D. Generative AI Revolutionizes Antibody Therapies Against Viruses, Including COVID-19 And Ebola, 2023.
32. Medicine, S. Generative AI Revolutionizes Antibiotic Development against Resistant Pathogens. https://www.news-medical.net/news/20240328/Generative-AI-revolutionizes-antibiotic-development-against-resistant-pathogens.aspx, 2024.
33. Genentech. AI and the Quest for New Antibiotics. https://www.gene.com/stories/ai-and-the-quest-for-new-antibiotics.
34. HHS Funds AI-enhanced Antibiotic Discovery Project | CIDRAP. https://www.cidrap.umn.edu/antimicrobial-stewardship/hhs-funds-ai-enhanced-antibiotic-discovery-project, 2024.
35. Sokolova, B. 9 Companies Using Artificial Intelligence to Fight Infectious Diseases. https://www.biopharmatrend.com/artificial-intelligence/9-companies-using-artificial-intelligence-to-fight-infectious-diseases-589/, 2022.
36. AI Agents in Healthcare: Benefits, Use Cases, Future Trends | SaM Solutions. https://sam-solutions.com/blog/ai-agents-in-healthcare/.
37. New AI Technology Can Detect Infections Early and Save Lives | Karolinska Institutet. https://news.ki.se/new-ai-technology-can-detect-infections-early-and-save-lives, 2025.
38. for Healthbeat, D.J.K.V. How AI Can Make Infectious Disease Surveillance Smarter, Faster, and More Useful. https://www.wftv.com/news/how-ai-can-make-infectious-disease-surveillance-smarter-faster-more-useful/2TRXO2QSCVMCVCIPXJYONMQ7RE/, 2025.
39. Artificial Intelligence Reimagines Infectious Disease Forecasting | PreventionWeb. https://www.preventionweb.net/news/artificial-intelligence-reimagines-infectious-disease-forecasting, 2025.
40. By. Harnessing AI to Model Infectious Disease Epidemics | Harvard T.H. Chan School of Public Health, 2025.
41. AI Agents for Infectious Disease Management | Bluebash. https://www.bluebash.co/services/artificial-intelligence/ai-agents/infectious-disease-management.

 doi:10.20944/preprints202509.1333.v1

42. AI Medicines Are Coming: Building the Foundations for Discovery's next Era. https://pharmaphorum.com/deep-dive/ai-medicines-are-coming-building-foundations-discoverys-next-era.
43. Digital Transformation and Artificial Intelligence | Sanofi. https://www.sanofi.com/en/our-science/digital-artificial-intelligence.
44. PhD, J.D.G. Drug-Resistant Bacteria Stymied by AI-Designed Antibiotics, 2024.
45. Shiwlani, A.; Kumar, S.; Qureshi, H.A. Leveraging Generative AI for Precision Medicine: Interpreting Immune Biomarker Data from EHRs in Autoimmune and Infectious Diseases. *Annals of Human and Social Sciences* **2025**, *6*, 244–260. https://doi.org/10.35484/ahss.2025(6-I)22.
46. How Does Generative AI Contribute to Early Disease Detection? - Ambilio. https://ambilio.com/how-does-generative-ai-contribute-to-early-disease-detection/.
47. ID Is Having a 'Wild West Moment' with AI. https://www.healio.com/news/infectious-disease/20240401/id-is-having-a-wild-west-moment-with-ai.
48. Research Assistant - Bohrium | AI for Science with Global Scientists. https://www.bohrium.com/paper-details/generative-artificial-intelligence-models-in-clinical-infectious-disease-consultations-a-cross-sectional-analysis-among-specialists-and-resident-trainees/10335998607978660 26-98026.
49. IQVIA Healthcare-grade AI®. https://www.iqvia.com/solutions/innovative-models/artificial-intelligence-and-machine-learning.
50. Trang, B. AI Agents in Health Care: Everything You Need to Know, but Didn't Know How to Ask, 2025.
51. The VR Hype Cycle: Lessons for the Age of AI. https://www.nngroup.com/articles/vr-hype-cycle-lessons-for-ai/.
52. Takyar, A. AI Agents for Healthcare: Applications, Benefits and Implementation, 2024.