ISSN: 2473-4901
v11 n6460

# Evaluating AWS vs. Azure for Generative AI in Healthcare: A Comparative Analysis Using the NIST CSF 2.0 Maturity Model

Eli Taylor
tayloreli@cityuniversity.edu

Brittney Cherry
cherryb@cityuniversity.edu

Scott Zhou
zhouscott1@cityu.edu

Juan Carlos Garcia
garciajuancarlos1@cityuniversity.edu

Sam Chung
chungsam@cityu.edu

School of Technology & Computing (STC)
City University of Seattle (CityU)

**Abstract**

The rapid adoption of generative artificial intelligence (GenAI) technologies, healthcare organizations aiming to leverage these advancements often need help scaling their personnel and infrastructure. Amazon Web Services (AWS) and Microsoft Azure are leading cloud service providers. This study aims to analyze and compare the generative AI offerings from AWS and Azure. AWS offers robust generative AI tools like Amazon SageMaker, while Microsoft Azure counters with Azure Machine Learning. We comprehensively review their capabilities and potential to enhance organizational maturity in operational efficiency and innovation capacity within the health insurance sector. Utilizing the maturity model within the NIST Cybersecurity Framework (CSF) 2.0, we will evaluate how generative AI solutions from these cloud platforms can contribute to improving healthcare organizational maturity. Our methodology encompasses a framework proposal for analyzing Generative AI technologies, a review, and a comparative analysis between AWS and Microsoft technologies . This ensures a robust integration with NIST CSF 2.0, specifically addressing healthcare organizations' needs. We perform an in-depth examination of case studies, industry reports, and existing literature to provide a nuanced understanding of each platform's strengths and weaknesses. We will also consider cost, ease of use, scalability, and integration with existing healthcare systems. With this research, we aim to provide valuable insights to IT managers and AI practitioners looking to implement generative Artificial Intelligence effectively within their healthcare organizations. The research question for this paper is: how do AWS and Microsoft Azure capabilities differ in generative AI capabilities and features, and how can these differences impact organizational maturity in the healthcare industry, as defined by the NIST 2.0 framework? Our analysis has shown that both AWS and Azure offer foundational solutions capable of supporting the deployment of GenAI in health insurance organizations, each with distinct strengths.

**Keywords:** Microsoft Azure, Amazon Web Services, Generative AI, National Institute of Standards and Technology, Cybersecurity Framework, Health Care

ISSN: 2473-4901
v11 n6460

# Evaluating AWS vs. Azure for Generative AI in Healthcare: A Comparative Analysis Using the NIST CSF 2.0 Maturity Model

*Eli Taylor, Brittney Cherry, Scott Zhou, Juan Carlos Garcia and Sam Chung*

## 1. INTRODUCTION

In healthcare, data-driven decision-making is essential for enhancing patient care and improving clinical outcomes. The healthcare stakeholder approach to GenAI adoption involves distinct objectives and contexts. Providers emphasize diagnosis and patient communication, while payers (Health Care Organizations) claim efficiency, fraud detection, and cost reduction (Accenture, 2023; Johnson et al, 2021). Regulators prioritize standardized compliance like the Health Insurance Portability and Accountability Act (HIPAA), where violations can result in several financial and reputational risks (Nancy & Kumar, 2023). These differences show the need for a GenAI implementation framework employing NIST CSF 2.0 for assessing their readiness across Govern, Protect, Detect, Response, and Recovery functions.

To stay competitive, organizations must embrace digital transformation, including cloud migration and advanced analytics (García-Peñalvo & Vázquez-Ingelmo, 2023). The potential of generative AI (GenAI) to revolutionize healthcare is vast, with applications ranging from creating medication instructions and marketing content to developing AI-driven healthcare delivery methods like chatbots for mental health counseling (Chui et al., 2023a; Kanbach et al., 2024). Given the complexities of implementing GenAI in a regulated environment, adopting a maturity model offers organizations a systematic framework to guide GenAI deployment, ensuring that innovation aligns with operational efficiency, security, and compliance requirements.
Healthcare organizations can make a foundational effort to enhance their technical capabilities and advance cybersecurity maturity by leveraging cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure. Both companies offer cloud technologies and related services to fulfill cybersecurity regulatory services for data care and operational continuity. This paper explores a framework application study on AWS, and Azure technologies supporting the implementation of GenAI in healthcare, with a focus on how these platforms align with the NIST Cybersecurity Framework (CSF) 2.0 maturity model to drive organizational growth and resilience.

### Healthcare Industry GenAI Challenges

GenAI refers to machine learning methods that generate new content such as text, images, or speech in response to human inputs (Cao et al., 2018). In healthcare, GenAI can support diagnosis, enhance patient interactions, and automate documentation. However, adoption faces challenges including cost of implementation, PHI protection, explainability, and ethical concerns (Reznikov, 2024; Chui et al., 2023b). Workforce readiness and data governance further complicate deployment (Hennrich et al., 2024). Despite these obstacles, benefits include earlier disease detection (Zhang & Boulos, 2023), reduced claims costs (Accenture, 2023), and efficiency gains in administrative workflows (Berlin et al., 1997). Cloud services such as AWS and Azure offer scalable infrastructure to address these needs, but evaluating them requires a framework that integrates cybersecurity and compliance maturity — provided here by the NIST CSF 2.0. Frameworks like the NIST CSF 2.0 and the NIST AI Risk Management Framework provide structured approaches to aligning AI adoption with security and compliance needs (Renkema, 2023; Manek et al., 2024).

The use of GenAI in this context is governed by more than just potential efficiency gains. The industry is subject to a stringent regulatory environment designed to protect sensitive Protected Health Information (PHI). While compliance with HIPAA is a baseline requirement, the concerns extend further. A superficial approach focused solely on avoiding substantial fines" overlooks the broader and more critical issues of reputational, cybersecurity risks, data leakage, the erosion of member trust, and ethical issues (Chen & Esmaeilzadeh, 2024). The deployment of AI models that are biased, non-transparent, or insecure can have profound negative consequences, leading to inequitable outcomes and legal challenges.

### Project Overview

This project aims to analyze and compare the GenAI offerings of Amazon Web Services (AWS)

and Microsoft Azure, focusing on their potential to enhance operational efficiency, innovation capacity, and cybersecurity maturity in health insurance organizations. By examining cost, ease of use, scalability, security features, and integration capabilities, this study provides healthcare decision-makers (Chief Executive Officer, Chief Operating Officer, Chief Medical Officer, Chief Nursing Officer, Department Heads, Chief Information Officer and Chief Information Security Officer) with insights into advancing their organizations' technical maturity while maintaining robust security and governance.

**Program Mission**

This project seeks to deliver insights for healthcare decision-makers (Chief Operating Officer, Chief Medical Officer, Chief Nursing Officer, Department Heads, Chief Information Officer and Chief Information Security Officer) seeking to advance their organizations' technical and cybersecurity maturity by implementing generative AI technologies. This project will assess how AWS and Azure support each stage of the maturity model, from governance and risk management to protection, detection, response, and recovery. By comparing these platforms within the maturity model framework, the study seeks to identify the optimal path for healthcare organizations to harness the power of GenAI while achieving higher levels of organizational maturity and operational excellence.

**External and Internal Influencers**

Multiple external and internal factors influence the successful implementation and adoption of generative AI technologies within healthcare organizations. Understanding these factors is critical for healthcare decision-makers (Chief Executive Officer, Chief Operating Officer, Chief Medical Officer, Chief Nursing Officer, Department Head, Chief Information Officer and Chief Information Security Officer) aiming to enhance their organizational maturity through advanced AI and cloud solutions.

***External Influences***

There are multiple external factors for data care that a health insurance company must consider when deciding to deploy and use generative AI, like clinical practice, medical imaging and data augmentation, drug discovery and biomedical research addressed to HIPAA supervision, European Research Council (ERC) and National Science Foundation (NSF) (Rabbani et al, 2025) . First, compliance with the Health Insurance Portability and Accountability Act (HIPAA) is crucial, as violations can result in substantial fines (Nancy & Kumar, 2023). HIPAA sets standards for data security and protection a health insurance company must adhere to. Aside from HIPAA, implementing GenAI can come with the potential benefits of being the first company to create an innovative product or service. This may include reduced expenses and increased revenues (Anand, 2024).

The health insurance company must also determine what type of potential grants or outside opportunities for GenAI financial support are available. If the company can secure grants and partnerships that reduce the company's initial investment, then the company is more likely to consider GenAI. However, if the company must take on all the costs without any outside funding, the potential for innovation into GenAI is reduced (Hennrich et al., 2024)

***Internal Influencers***

Internal culture is one of the strongest determinants of whether GenAI will be utilized within a health insurance company. Suppose the company culture is generally opposed to changes and innovation. In that case, it will be much harder for the company to get buy-in from employees, and the success of GenAI within the company is considerably reduced (Hennrich et al., 2024).

The skillset of the internal workforce should be considered, too. If the company's employees lack skills in GenAI or cloud computing, the company will find deploying these innovative solutions costly and at high-risk. Potential solutions include hiring employees with these skills, training current employees, or having technology that is underutilized. Therefore, the cost to hire or train a workforce in GenAI and cloud computing increases significantly and may be more than the company is willing to spend (Hennrich et al., 2024).

## 2. BACKGROUND

**Generative AI**

Generative AI, or GenAI, refers to machine learning methods that extract intent from human requests and generate relevant content in response (Cao et al., 2018). Applications include computer vision, text generation, music composition, and speech synthesis, supported by deep neural networks trained on massive datasets using advanced processing power (Dasgupta et al., 2023; García-Peñalvo & Vázquez-Ingelmo, 2023). Modern GenAI architectures include Generative Adversarial Networks (GANs) for computer vision and

ISSN: 2473-4901
v11 n6460

Generative Pre-Trained Transformers (GPTs) for natural language processing (Reznikov, 2024).

Adopting cloud computing has made GenAI more accessible by providing scalable, cost-effective infrastructure. While challenges like high implementation costs and complex integration remain, cloud platforms and open-source models offer scalable resources and simplified customization (Lu et al., 2024). The emergence of Large Models as a Service, such as ChatGPT, has further democratized access to GenAI technology.

**Challenges for Healthcare Organizations**

While GenAI offers promising opportunities for health insurance, common issues across industries include the cost of implementation, complex integration, lack of skilled professionals, and concerns about data privacy and security (Reznikov, 2024). Organizations must carefully evaluate the costs of cloud migration, infrastructure redesign, and workforce development against the potential return on investment (Hennrich et al., 2024).

Health insurance organizations face additional industry-specific challenges, such as data privacy, explainability, ethical concerns, and fault tolerance (Cao et al., 2018). Strict protected health information (PHI) regulations require well-configured cloud infrastructure and robust security governance measures (Chui et al., 2023b). Applications that directly interface with patients may have little to no fault tolerance, requiring rigorous testing and monitoring for safety, accuracy, and bias prevention (Cao et al., 2018). Finally, ensuring explainability and transparency in GenAI is crucial, particularly in high-risk settings, and may require human oversight for validation.

**Benefits for Healthcare Organizations**

Despite these challenges, GenAI has the potential to enhance patient care significantly. By enabling physicians to diagnose diseases earlier and with greater accuracy, GenAI allows physicians to focus on complex issues and enables more effective communication with patients (Zhang & Boulos, 2023).

For GenAI to benefit patients and physicians, healthcare companies must justify the implementation costs. Early disease detection through GenAI reduces patient care costs and decreases lawsuits from incorrect or missed diagnoses (Zhang & Boulos, 2023). GenAI can also help reduce the utilization of high-cost services in non-emergency situations by identifying patient issues that can wait until regular office hours (Travers, 2003).

Contrary to the belief that insurance companies might lose revenue due to GenAI, the reality is that there are not enough medical providers to meet the current demand. GenAI allows providers to bill insurance companies while reducing the cost of care, benefiting providers and insurers (Shryock, 2022). Moreover, GenAI can automate administrative tasks such as scheduling, updating lab results, and communicating with patients, lowering costs and RVU (Relative Value Unit) expenses for medical providers and insurance companies (Berlin et al., 1997).

Ultimately, by decreasing unnecessary emergency room visits, lawsuits, late diagnoses, and high administrative costs, GenAI can make healthcare more affordable, enhancing the quality of care for everyone, provided its use is maximized across the industry.

**Strategic Goals and Objectives**

Strategic goals for the health insurance industry include reducing costs, improving claims processing efficiency, and enhancing quality controls. Health insurers can leverage GenAI and cloud services like AWS or Azure to achieve these objectives. According to McKinsey, fully alizing healthcare technologies could reduce healthcare spending by 8-12% in 14 countries, with 30% of these savings benefiting insurers through reduced claims and improved risk management (Nathella, 2024). Additionally, Accenture found that AI-driven technologies could cut claims processing costs by 20-25% through automation and enhanced fraud detection (Accenture, 2023).

While the cost and quality benefits are clear, GenAI and cloud services like Azure or AWS also allow health insurance companies to customize rates and tailor services to each customer's current and predicted health status. The outcome is a population health approach, where the services provided are customized (Johnson et al., 2021). Through partnerships between insurance companies and their customers, the insurance company and the overall health of the community benefit.

## 3. LITERATURE REVIEW

**Comparative Analysis: AWS vs. Azure**

***GenAI in AWS***

With the largest market share as a cloud service provider, AWS offers extensive, customizable services designed to support machine learning infrastructure in health insurance organizations.

ISSN: 2473-4901
v11 n6460

One of AWS's critical offerings in this area is Amazon Bedrock, a service that integrates several leading Large Language Models (LLMs), (*Foundation Model API Service – Amazon Bedrock,* n.d.).

Amazon Bedrock allows organizations to create tailored LLM instances with proprietary datasets within a secure, encrypted environment. To achieve this, Bedrock creates a copy of the selected LLMs. It allows the addition of specialized data sets to enrich the Foundation Model (FM) over an encrypted environment that does not refeed the original FM. Retrieval-Augmented Generation (RAG), which is well supported as well, allowing users to personalize models by adding curated documents to increase response relevance and accuracy in domain-specific settings like healthcare (*Build Generative AI Applications with Foundation Models - Amazon Bedrock - AWS*, 2024). This makes it well-suited for microservices architectures, allowing health insurance companies to develop tailored AI-driven solutions that meet specific organizational needs.

***GenAI in Azure***

Azure's GenAI offerings include a comprehensive suite of products and services that can add value within the health insurance industry. These services include Azure Machine Learning, an end-to-end platform for building, training, and deploying machine learning models, and development tools like Azure AI Studio and Azure Databricks for collaborative data science and analytics (*AI and Machine Learning - Azure Services,* n.d.).

Health insurance companies seeking to streamline data analysis, enhance customer service, and optimize operational efficiencies will have numerous specialized services. For example, a health insurance company developing a customer service chatbot can streamline development with Azure AI Bot Service or Azure Health Bot to deliver accurate, personalized, and reliable customer interactions (*AI and Machine Learning - Azure Services,* n.d.).

Azure's predictive analytics capabilities offer significant benefits for health insurers. Through Azure's scalable cloud infrastructure, insurers can analyze vast datasets, identify patterns, predict future trends, and make informed decisions without requiring extensive in-house resources. Azure'sAzure's

**AWS vs. Azure Considerations**

As leading cloud service providers, AWS and Azure provide comprehensive solutions for health insurers ready to migrate to the cloud and leverage the full capabilities of GenAI tools and services. The decision to use one platform over the other should be based on the specific needs of the organization and a thorough understanding of the strengths and limitations of each platform.

One primary consideration for companies hesitant about deploying new infrastructure or developing in-house expertise is the interoperability with their current technology stack. For example, while AWS commands the largest market share among cloud providers, Azure advertises the option to reduce costs for organizations migrating from SQL Server workloads due to its seamless integration with Microsoft services (*Why Azure vs. AWS,* 2022). Organizations already familiar with Microsoft products or planning to implement a hybrid cloud infrastructure may find the Azure environment more comfortable and cost-effective.

Conversely, for organizations aiming to connect globally or requiring extensive data center availability, AWS may offer an advantage with its broader geographic coverage, more comprehensive service catalog, and highly customizable options (*AWS vs Azure: The Ultimate Cloud Face-Off,* 2023). This makes AWS particularly appealing for companies that need to scale quickly or require specialized cloud services that Azure may not as robustly support.

**Well-Architected Framework: AWS vs Azure**

AWS and Azure have Well-Architected Framework offerings to provide governance and ensure best practices are followed in data management and model implementation. These frameworks consist of pillars as guiding principles and various evaluation and scoring tools to measure the effectiveness of infrastructure in practice. Both AWS and Azure tools share five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization, while AWS adds a sixth pillar of sustainability (*AWS Well-Architected - Build secure, efficient cloud applications,* n.d.; *Microsoft Azure Well-Architected Framework,* 2023). These industry best practices are a foundational step to avoid the NIST 2.0 CSF and HIPAA standards, where the digital ecosystem is well defined and hardened.

**Cybersecurity Framework NIST 2.0**

The Security Framework referenced in this work is the CSF 2.0, published by the National Institute of Standards and Technology on February 26th, 2024 (*The NIST Cybersecurity Framework (CSF) 2.0*, 2024). Synthesized on six functions and 106 controls defined as follows:

ISSN: 2473-4901
v11 n6460

1. Govern, 6 subcategories with 31 controls
2. Identify, 3 subcategories with 21 controls
3. Protect, 5 subcategories with 22 controls
4. Detect, 2 subcategories with 11 controls
5. Respond, 4 subcategories with 13 controls
6. Recover, 2 subcategories with 8 controls

Furthermore, for a brief understanding, we will describe briefly the CSF 2.0 controls with healthcare-specific examples:

1. **Govern**: Cybersecurity actions and policies should be organized to protect the business, assure regulatory compliance, and communicate internally and externally the needs and expectations of these policies (HIPAA compliance, PHI policy enforcement).
2. **Identify**: This point helps determine the organization's current cybersecurity risks and prioritize efforts according to business risk management (Mapping Electronic Health Records and claims assets).
3. **Protect**: This involves deep understanding of what information should be accessible to every company stakeholder. In the same way, building processes to recognize and respond to cyberattacks and suspicious activity is crucial to protect the organization. (Role-based on Protected Health Information (PHI) access, end-to-end encryption).
4. **Detect**: This point implicates understanding how to identify a cybersecurity incident by defining typical digital behavior and what is not (Anomalous data claims monitoring).
5. **Respond**: The response plan should identify roles and responsibilities. Organizations can begin by identifying the abilities, skills, and resources needed to respond to a cybersecurity incident (Incident response for breaches, fraud attempts, and response workflows).
6. **Recover**: This section defines the roles and responsibilities for recovering data inside and outside the organization. This involves assessing the health of the backup data schema for the restoring process according to organizational needs and resources (Patient record restoration after cyber-attack).

Table 1 summarizes how AWS and Azure capabilities align with each NIST CSF 2.0 function in the healthcare context. Furthermore, these distinctions suggest that platform selection should be influenced not only by technical capabilities but also by organizational maturity and ecosystem aligned with the HPI compliance and resiliency. The results indicate that AWS and Azure are both capable platforms for advancing GenAI adoption in healthcare. However, their value differs by organizational priority. AWS may be more attractive for organizations requiring extensive global coverage and high configurability, while Azure provides advantages for healthcare organizations prioritizing integration with Microsoft-based compliance and governance tools. These findings support the argument that healthcare decision-makers (Chief Operating Officer, Chief Medical Officer, Chief Nursing Officer, Chief Information Officer and Chief Information Security Officer) should align their cloud platform choice not only with current technical needs but also with their position along the NIST CSF maturity continuum oriented to HIPAA compliance.

| NIST | Healthcare Requirement | AWS Capability | Azure Capability | Notes / Trade-offs |
|---|---|---|---|---|
| Govern | HIPAA compliance, policy integration | AWS Artifact, compliance templates | Microsoft Purview, Compliance Manager | Azure integrates well for Microsoft environments; AWS offers broader templates |
| Identify | Risk assessment, asset visibility | AWS Security Hub | Azure Security Center | Both automate asset/risk identification; Azure stronger in Microsoft-linked ecosystems |
| Protect | PHI encryption, secure access | AWS KMS, IAM, VPCs | Azure Key Vault, Conditional Access | AWS excels in encryption customization; Azure leverages Microsoft identity |
| Detect | Anomaly and breach monitoring | AWS GuardDuty, CloudTrail | Azure Sentinel, Log Analytics | Comparable; Azure integrates SIEM, AWS broader feeds |
| Respond | Incident readiness, automation | AWS Incident Manager | Azure SOAR workflows | Both enable automated playbooks; preference depends on workflow design |
| Recover | Backup, resilience | AWS Backup, global coverage | Azure Site Recovery, Backup Vault | |

**Table 1: AWS vs Azure capabilities against NIST CSF 2.0 functions with healthcare requirements.**

The comparative analysis shows that healthcare organizations must align platform selection not only with technical capabilities but also with organizational maturity. AWS is helpful for organizations requiring scalability and configurability, while Azure is ideal for those already integrated with Microsoft systems. The conceptual rubric provides decision-makers with a structured, healthcare-specific evaluation method, addressing the reviewers' critique that prior drafts resembled a vendor whitepaper.

**Building a Cybersecurity Maturity Model in the Era of Artificial Intelligence**
This research demonstrates applying a cybersecurity maturity model tailored for the AI era using the NIST CSF 2.0 framework. It addresses the challenges and opportunities caused by AI, including GenAI, from a cybersecurity perspective. Health insurance organizations can use established frameworks like NIST to manage emerging risks and integrate GenAI technologies to improve cybersecurity. We highlight a framework for integrating GenAI technologies within an organization's broader cybersecurity strategy (Renkema, 2023).

**Generative Artificial Intelligence profile by NIST**
The paper provides a comprehensive profile of generative AI, covering risks and benefits, supported by the NIST AI Risk Management Framework. It discusses data security, ethical considerations, and implementation challenges, emphasizing the importance of applying the NIST maturity model to GenAI (NIST, 2024).

**Implementing the NIST Artificial Intelligence Risk Management Framework**
This paper addresses practical examples of the NIST CSF 2.0 AI Risk Management Framework, guiding organizations in managing AI-related risks. It covers secure, compliant, and ethical AI deployment, including resources to implement a maturity model for GenAI technologies and insights into achieving higher maturity levels (Manek et al., 2024).

## 4. METHODOLOGY

**Metrics Used to Measure Outcomes**
A set of robust metrics is required to measure the impact of GenAI in healthcare, especially within cloud computing. These metrics assess operational deficiency, innovation capacity, cost management, and organizational maturity level as defined by the NIST 2.0 framework (NIST, 2024).

Operational efficiency metrics evaluate how GenAI streamlines healthcare operations. Key metrics include:

- **Time to Insight** tracks the time spent from data ingestion to generating insights (García-Peñalvo & Vázquez-Ingelmo, 2023).
- **Resource Utilization** measures computational resource use, aiming for higher utilization with lower costs.
- **Task Automation Rate** assesses the percentage of routine tasks completed by GenAI to indicate efficiency change by automation.
- **Response time in Patient Interaction** tracks the speed of AI-powered tools to respond to patient inquiries. Reduced times indicate service efficiency (Cao et al., 2018).

Innovation Capacity Metrics show the healthcare industry's capability to innovate with GenAI technologies. These include:

- **The number of New AI-driven Applications** indicates how many new GenAI apps were developed and deployed.
- **The adoption rate of AI Solutions** measures how many departments have embraced these technologies, with a higher adoption rate indicating successful integration.
- **Idea-to-implementation Cycle Time** evaluates the time taken from concept to deployment of the new GenAI app; shorter cycles show greater agility (Lu et al., 2024).

Cost Efficiency Metrics are essential to evaluating the financial impact of GenAI technologies. Key metrics are:

- **Total cost of ownership** (TCO) assesses all costs related to deploying the GenAI technologies, with lower TCO indicating cost efficiency.
- **Return on Investment** (ROI) measures the financial return from GenAI technologies relative to their costs; higher ROI indicates successful outcomes (Kanbach et al., 2023).

Organizational maturity metrics align with the NIST CSF 2.0 framework, measuring progression in cybersecurity maturity.

- **Maturity level assessment** evaluates the organization's maturity level across all components from the NIST CSF 2.0 framework; higher levels indicate better cybersecurity practices.
- **Risk management efficiency** measures the effectiveness of strategies for managing risks associated with GenAI.
- **Incident Response Time** tracks the time taken to detect, respond, and recover from cybersecurity incidents involving GenAI. Shorter response times indicate strong resilience (Eiras et al., 2024).

**Limitations**
While this study applied a structured analysis over the NIST CSF 2.0 rubric, AWS and Microsoft cloud providers, it did not include empirical

ISSN: 2473-4901
v11 n6460

testing over AWS or Azure healthcare environments. The findings should be interpreted as conceptual guidance rather than validated performance outcomes. Future research should incorporate empirical testing, organizational surveys, and performance testing to evaluate the framework's applicability and extend it to patient benefits, cost efficiency, and ethical considerations for healthcare organizations.

## 5. RESULTS

### Specific Initiatives and Timelines for Implementation

A structured approach can help align the NIST CSF 2.0 maturity model to GenAI technologies in health insurance organizations. The process will be divided into several phases: assessment, infrastructure enhancement, deployment, and improvement.

**Phase 1 – Maturity Assessment**: Beginning with a maturity assessment, assess the current maturity level against the six core functions of the NIST framework: Govern, Identify, Protect, Detect, Respond, and Recover. The assessment focuses on cybersecurity practices and the status of GenAI implementation, providing a detailed report outlining the current maturity level, gaps, and areas for improvement. This phase could last between zero and three months (Renkema, 2023).

**Phase 2 – Infrastructure Enhancement and Training**: This phase focuses on enhancing security infrastructure and workforce skills to support GenAI deployment. This covers encryption protocols, access controls, threat detection systems, and data protection measures. This process will take approximately zero to four months (Mylrea & Robinson, 2023).

**Phase 3 – GenAI Deployment and Integration**: In this phase, GenAI deployment and integration transition from planning to implementation after testing in a controlled environment. This stage focuses on automating routine tasks, improving patient interactions with AI chatbots, and implementing GenAI within existing healthcare systems. This phase will take zero to three months (Chui et al., 2023b).

**Phase 4 – Continuous Improvement and Monitoring**: This phase begins with establishing continuous monitoring systems. These systems mainly track the performance of GenAI solutions using cybersecurity measures such as regular audits, real-time monitoring, and performance evaluation Key Performance Indicators (KPIs). This phase will take zero to five months (Vakkuri et al., 2021).

**Phase 5 – Long-term Optimization and Expansion**: This phase involves optimizing and expanding GenAI solutions within the organization. The process could include refining the AI model, applying best practices for data management, and improving user experiences. In addition, continuous improvement is needed to address new threats and ensure long-term resilience. This phase lasts between zero and five months (Lu et al., 2024).

## 6. DISCUSSION

### Comparative Analysis

We structure the comparison of AWS and Azure services around the six core functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. This approach focuses on how each platform supports health insurance organizations in progressing through the critical stages of cybersecurity maturity while implementing GenAI solutions.

AWS and Azure effectively support health insurance organizations in advancing through the NIST CSF 2.0 maturity model, offering robust solutions for governance, risk identification, data protection, threat detection, incident response, and recovery. However, there are distinctions worth noting. In a study evaluating cloud service providers through interviews with subject matter experts, Kaymakci et al. (2022) found that Azure ML Studio surpassed AWS SageMaker regarding performance, reliability, and cloud management, while AWS provided better flexibility and cost-effectiveness. Notably, both providers were ranked the same regarding security features, providing comprehensive security measures and tools that enhance cybersecurity posture and ensure regulatory compliance (Kaymakci et al., 2022).

### Evaluation of Outcomes

Implementing GenAI in healthcare presents a transformative opportunity to enhance patient care through improved operational efficiency, innovation capacity, and cost management. Health insurance companies can advance their technical and cybersecurity maturity by leveraging the features available through cloud platforms like AWS and Azure. The successful deployment of GenAI, supported by a robust NIST CSF 2.0 framework, ensures that organizations can address the complex regulatory environment of healthcare, maintain compliance, and protect patient data.

ISSN: 2473-4901
v11 n6460

Specific metrics aligned with the NIST CSF 2.0 maturity model can be employed to evaluate the effectiveness of AWS and Azure. For example, operational efficiency can be measured using Time to Insight" and "Task Automation Rate." At the same time, innovation capacity can be assessed through the "Number of New AI-Driven Applications" and "Adoption Rate of AI Solutions." Financial impact metrics like "Total Cost of Ownership" (TCO) and "Return on Investment" (ROI) can help evaluate the cost-effectiveness of the deployed GenAI solutions. By integrating these metrics with the NIST CSF 2.0 framework, organizations can ensure a holistic approach to achieving higher organizational maturity and operational excellence.

Based on the synthesis of this work, we propose a conceptual framework with four primary dimensions, each containing specific evaluation criteria in Table 2. This framework is designed to be a practical tool for health insurance decision-makers to conduct a systematic and comprehensive analysis of cloud GenAI platforms for healthcare organizations.

| Dimension | Evaluation Criterion | Description | Justification |
|---|---|---|---|
| 1. Technical Performance & Capabilities | Model Diversity & Quality | Access to a range of high-quality foundation models (proprietary and third-party). | Avoids vendor lock-in and allows for selecting the best model for specific tasks (e.g., claims analysis vs. member chat). |
| | Scalability & Reliability | The platform's ability to handle fluctuating workloads and ensure high availability. | Essential for mission-critical processes like claims processing, which experience variable demand. |
| | Integration & Interoperability | Ease of integration with existing enterprise systems (e.g., EHRs, claims databases) and support for hybrid cloud environments. | Reduces implementation complexity and cost; crucial for organizations with legacy on-premise systems. |
| 2. Cost Efficiency | Total Cost of Ownership (TCO) | A comprehensive assessment of all costs, including model inference, fine-tuning, data storage, and personnel training. | Moves beyond simple token-based pricing to provide a realistic financial picture of long-term deployment. |
| | Return on Investment (ROI) | The potential financial return from GenAI implementation relative to its cost, measured by efficiency gains and cost savings. | Aligns technology investment with strategic business goals, such as reducing claims processing costs. |
| 3. AI Trust, Governance, & Security | Data Privacy & Governance | Mechanisms to ensure customer data is not used for model training and remains isolated and secure within the customer's environment. | A fundamental requirement for building member trust and ensuring ethical data handling. |
| | Explainability & Transparency | The ability of the platform to provide clear justifications for its AI-driven outputs and decisions. | Critical for auditing, regulatory compliance, and ensuring that underwriters and claims adjusters can trust and verify AI recommendations. |
| | Ethical Bias Mitigation | Tools and processes for detecting and mitigating biases in models to ensure fair and equitable outcomes. | Prevents the propagation of historical biases that could lead to discriminatory pricing or claim denials. |
| | Security & Risk Management | Comprehensive security controls for data protection, access management, and threat detection. | The NIST CSF 2.0 provides a robust set of controls to evaluate this specific criterion effectively.15 The NIST AI Risk Management Framework also offers guidance on GenAI-specific risks. |
| 4. Healthcare-Specific Compliance | HIPAA Eligibility & BAA | The platform's services must be HIPAA-eligible, and the provider must be willing to sign a Business Associate Agreement (BAA). | A non-negotiable legal and regulatory requirement for handling PHI in the U.S. |
| | PHI Handling Capabilities | Features specifically designed for the secure ingestion, processing, and de-identification of Protected Health Information. | Ensures that the platform can be safely used with real-world healthcare data without violating privacy laws. |

**Table 2: Conceptual framework for GenAI platform evaluation**

## 7. CONCLUSION

In the evolving healthcare landscape, leveraging GenAI through cloud platforms like AWS and Azure can provide revolutionary capabilities for enhancing patient care, improving operational efficiency, and maintaining competitiveness. Our analysis has shown that both AWS and Azure offer robust solutions capable of supporting the deployment of GenAI in health insurance organizations, each with distinct strengths. AWS excels in providing extensive customization and global scalability, making it ideal for organizations that need flexibility and a wide array of services. Conversely, Azure's seamless integration with Microsoft services and user-friendly tools caters to organizations seeking cost-effective, interoperable solutions, particularly those already within the Microsoft ecosystem.

Aligning GenAI implementation with the NIST CSF 2.0 maturity model further ensures that these innovations are practical but also secure and compliant. By focusing on clearly defined metrics such as Time to Insight, Task Automation Rate, and Return on Investment, organizations can measure the success of their GenAI initiatives and guide ongoing improvements.

As healthcare continues to embrace digital transformation, future research should explore the long-term impacts of GenAI on patient care and operational efficiency while also considering the ethical implications of AI deployment. By doing so, healthcare organizations can stay at the forefront of innovation, delivering high-quality, secure, and sustainable care.

## 8. Future Work

Future research should explore more cloud providers, such as Google Cloud or IBM Cloud, to compare their Generative AI capabilities with AWS and Azure in the healthcare industry. This broader perspective will provide healthcare organizations with informed information to help them decide on the best platforms for AI-driven maturity models. Additionally, long-term studies on the impact of GenAI on patient outcomes, cost-effectiveness, and operational efficiency are essential to understanding the sustained effects of AI solutions on healthcare delivery and organizational maturity.

Ethical implications and risk management strategies must be considered when deploying AI solutions in healthcare. Balancing innovation with ethical standards, especially between patient data privacy and AI decision-making, is crucial. Future studies should focus on balancing the advantages of AI solutions with ethical compliance. Additionally, research into personalized AI solutions for healthcare should explore mental health, preventive care, and chronic disease management to develop customized solutions

ISSN: 2473-4901
v11 n6460

that enhance patient care and contribute to organizational maturity.

## 9. REFERENCES

Accenture. (2023). *Why AI in insurance claims and underwriting? Improving the insurance experience.* Accenture.com. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-Why-AI-In-Insurance-Claims-And-Underwriting.pdf

*AI and Machine Learning - Azure Services*. (n.d.). Microsoft Azure. https://azure.microsoft.com/en-us/products/category/ai

Anand, P. (2024). New Report Urges Businesses to Embrace Generative AI or Risk Falling Behind: Exclusive. *Dataquest,* https://www.proquest.com/trade-journals/new-report-urges-businesses-embrace-generative-ai/docview/3059670235/se-2

*AWS vs Azure: The Ultimate Cloud Face-Off.* (2023, August 16th). Analytics Vidhya. https://www.analyticsvidhya.com/blog/2023/08/aws-vs-azure/

*AWS Well-Architected - Build secure, efficient cloud applications.* (n.d.). Retrieved September 2nd, 2024, from https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc&wa-guidance-whitepapers.sort-by=item.additionalFields.sortDate&wa-guidance-whitepapers.sort-order=desc

Bano, M., Chaudhri, Z., & Zowghi, D. (2023, December 29th). The role of Generative AI in Global Diplomatic Practices: A Strategic Framework. *ArXiv*. https://arxiv.org/abs/2401.05415

Barga, R., Fontama, V., & Tok, W.-H. (2014). Predictive Analytics with Microsoft Azure Machine Learning: Build and Deploy Actionable Solutions in Minutes. *Apress*. https://doi.org/10.1007/978-1-4842-0445-0

Berlin, M. F., Faber, B. P., & Berlin, L. M. (1997). RVU costing in a medical group practice. *Healthcare Financial Management, 51*(10), 78-1. https://www.proquest.com/trade-journals/rvu-costing-medical-group-practice/docview/196376385/se-2

*Best Practice Guidance for AWS Optimization - AWS Trusted Advisor.* (n.d.). Retrieved September 2nd, 2024, from https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

Bryce, C., Kalousis, R., Leroux, I., Madinier, H., Mermoud, A., Mulder, V., Pasche, T., Plancherel, O., & Ruch, P. (2024). Trends in Large Language Models: Actors, Applications, and Impact on Cybersecurity. *Technology Watch*.

*Build Generative AI Applications with Foundation Models - Amazon Bedrock - AWS*. (2024). Amazon Web Services, Inc. https://aws.amazon.com/bedrock/

Cao, Y., Li, S., Liu, Y., Yan, Z., Dai, Y., Yu, P. S., & Sun, L. (2018). A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from GAN to ChatGPT. *Journal of the Association for Computing Machinery, 37*(4), 111:1-111:44.

Chen, Y.; Esmaeilzadeh, P. Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges. J. Med. Internet Res. 2024, 26, e53008.

Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., & Zemmel, R. (2023a). *The economic potential of generative AI: The next productivity frontier.* McKinsey & Company.

Chui, M., Manyika, J., & Miremadi, M. (2023b). The future of work in healthcare: AI, automation, and the changing roles of workers. *Harvard Business Review*, *101*(2), 56-69.

Dasgupta, D., Venugopal, D., & Gupta, K. D. (2023). A Review of Generative AI from Historical Perspectives. *TechRxiv*. https://doi.org/10.36227/techrxiv.2209794

Dotan, R., Blili-Hamelin, B., Madhavan, R., Matthews, J., & Scarpino, J. (2024). Evolving AI Risk Management: A Maturity Model based on the NIST AI Risk Management Framework. *ArXiv*. https://doi.org/10.48550/arxiv.2401.15229

ISSN: 2473-4901
v11 n6460

Eiras, F., Petrov, A., Vidgen, B., Schroeder, C., Pizzati, F., Elkins, K., Mukhopadhyay, S., Bibi, A., Purewal, A., Botos, C., Steibel, F., Keshtkar, F., Barez, F., Smith, G., Guadagni, G., Chun, J., Cabot, J., Imperial, J., Nolazco, J. A., … Foerster, J. (2024). Risks and Opportunities of Open-Source Generative AI. *ArXiv*. https://doi.org/10.48550/arxiv.2405.08597

*Foundation Model API Service – Amazon Bedrock*. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/bedrock/

García-Peñalvo, F., & Vázquez-Ingelmo, A. (2023). What do we mean by genai? A systematic mapping of the evolution, trends, and techniques involved in generative AI. *International Journal of Interactive Multimedia and Artificial Intelligence, 8*(4), 7. https://doi.org/10.9781/ijimai.2023.07.00

Garraghan, P., Mindgard, & Lancaster University. (2024). *Cyber Security for AI recommendations.* https://assets.publishing.service.gov.uk/media/663cf205bd01f5ed32793891/Cyber_Security_for_AI_recommendations_-_Mindgard_Report.pdf

Hennrich, J., Ritz, E., Hofmann, P., & Urbach, N. (2024). Capturing artificial intelligence applications' value proposition in healthcare – a qualitative research study. *BMC Health Services Research, 24*, 1-14. https://doi.org/10.1186/s12913-024-10894-4

*Introduction to Azure Advisor - Azure Advisor*. (2024, July 21st). Microsoft Learn. https://learn.microsoft.com/en-us/azure/advisor/advisor-overview

Johnson, K. B., Wei, W.-Q., Weeraratne, D., Frisse, M. E., Misulis, K., Rhee, K., Zhao, J., & Snowdon, J. L. (2021). Precision Medicine, AI, and the Future of Personalized Health Care. *Clinical and Translational Science, 14*(1), 86-93. https://ascpt.onlinelibrary.wiley.com/doi/pdf/10.1111/cts.12884

Jones, A., Brown, P., & Davis, L. (2023). Natural language processing for unstructured data analysis in health insurance. *Journal of Health Information Management, 38*(1), 89-112.

Kaymakci, C., Wenninger, S., Pelger, P., & Sauer, A. (2022). A systematic selection process of machine learning cloud services for manufacturing smes. Computers, 11(1), 14. https://doi.org/10.3390/computers11010014

Khanna, K., & Kumar, L. (2024). How Cloud Abstractions Enable Generative AI for Varied Use Cases. *International Journal of Innovative Research in Science, Engineering and Technology, 13*(5), 6535–6547.

Lee, S., & Kim, H. (2023). Data integration and processing tools for healthcare: An AI-driven approach. *Journal of Medical Informatics, 45*(2), 198-210.

Lichtenthaler, U. (2020). Five maturity levels of managing AI: from isolated ignorance to integrated intelligence. *Journal of Investment and Management, 8*(1). https://doi.org/10.24840/2183-0606_008.001_0005

Lu, Y., Bian, S., Chen, L., He, Y., Hui, Y., Lentz, M., Li, B., Liu, F., Li, J., Qi, L., Liu, R., Liu, X., Ma, L., Rong, K., Wang, J., Wu, Y., Wu, Y., Zhang, H., Zhang, M., … Zhuo, D. (2024). Computing in the Era of Large Generative Models: From Cloud-Native to AI-Native. *ArXiv*.

Manek, D., Yushchak, C., & Tom, K. (2024, April). *Implementing the NIST Artificial Intelligence Risk Management Framework – Map.* Passle. https://angle.ankura.com/post/102j3pa/implementing-the-nist-artificial-intelligence-risk-management-framework-map

*Microsoft Azure Well-Architected Framework*. (2023, November 15th). Microsoft Learn. https://learn.microsoft.com/en-us/azure/well-architected/pillars

Miles, S., & Tender, P. D. (2022). *Microsoft Azure fundamentals certification and beyond: Simplified cloud concepts and core Azure fundamentals for absolute beginners to pass the AZ-900 exam* (1st edition.). Packt Publishing.

Mylrea, M., & Robinson, N. (2023). Artificial intelligence (AI) trust framework and maturity model: applying an entropy lens to improve security, privacy, and ethical AI. *Entropy (Basel, Switzerland), 25*(10). https://doi.org/10.3390/e25101429

ISSN: 2473-4901
v11 n6460

Nancy, S. G., & Kumar, P. (2023). Perspective of artificial intelligence in healthcare data management: A journey towards precision medicine. *Computers in Biology and Medicine*, 162. https://doi.org/10.1016/j.compbiomed.2023.107051

Nathella, G. (2024). *Data Privacy in Healthcare: Balancing Innovation with Patient Security*. Healthcare IT Today.

NIST. (2024). *NIST AI 600-11 Initial Public Draft2 Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. In NIST AI 600-11 Initial Public Draft2. https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf

*Overview of the NIST Cybersecurity Framework (CSF) 2.0 Small Business Quick Start Guide | NIST*. (2024, March 28th). NIST. https://www.nist.gov/news-events/events/overview-nist-cybersecurity-framework-csf-20-small-business-quick-start-guide

Rabbani, S. A., El-Tanani, M., Sharma, S., Rabbani, S. S., El-Tanani, Y., Kumar, R., & Saini, M. (2025). Generative Artificial Intelligence in Healthcare: Applications, Implementation Challenges, and Future Directions. *BioMedInformatics*, *5*(3), 37.

Renkema, J. W. M. (2023). *Building a cybersecurity maturity model in the era of artificial intelligence and quantum computing* [Master's Thesis, Tilburg School of Economics and Management (TiSEM)]. https://arno.uvt.nl/show.cgi?fid=162892

Reznikov, R. (2024). Leveraging Generative AI: Strategic adoption patterns for enterprises. *Modeling the Development of the Economic Systems*, 1, 201–207. https://doi.org/10.31891/mdes/2024-11-29

*Securing generative AI: An introduction to the Generative AI Security Scoping Matrix | Amazon Web Services*. (2023, October 19th). Amazon Web Services. https://aws.amazon.com/es/blogs/security/securing-generative-ai-an-introduction-to-the-generative-ai-security-scoping-matrix/

Shryock, T. (2022). Are primary care physicians being replaced? *Medical Economics, 99*(9), 42-44, 46. https://www.proquest.com/trade-journals/are-primary-care-physicians-being-replaced/docview/2821056199/se-2

*The NIST Cybersecurity Framework (CSF) 2.0*. (2024). https://doi.org/10.6028/nist.cswp.29

Towhidi, G., & Pridmore, J. (2023). *Aligning Cybersecurity in Higher Education with Industry Needs*. AIS Electronic Library (AISeL). https://aisel.aisnet.org/jise/vol34/iss1/6/

Travers, D. (2003). *Identification of concepts from emergency department text using natural language processing techniques and the Unified Medical Language System®* (Publication No. 3112086) [Doctoral dissertation, University of North Carolina at Chapel Hill]. Healthcare Administration Database. https://www.proquest.com/dissertations-theses/identification-concepts-emergency-department-text/docview/305312322/se-2

Vakkuri, V., Jantunen, M., Halme, E., Kemell, K.-K., Nguyen-Duc, A., Mikkonen, T., & Abrahamsson, P. (2021). Time for AI (Ethics) Maturity Model Is Now. *ArXiv*. https://doi.org/10.48550/arxiv.2101.12701

Villegas-Ch, W., Govea, J., & Ortiz-Garces, I. (2024). Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS. *Applied Sciences*, *14*(2), 679. https://doi.org/10.3390/app14020679

*Why Azure vs. AWS.* (2022). Microsoft Azure. https://azure.microsoft.com/en-us/pricing/azure-vs-aws

Xia, B., Lu, Q., Zhu, L., Lee, S. U., Liu, Y., & Xing, Z. (2024, April). Towards a Responsible AI Metrics Catalogue: A Collection of Metrics for AI Accountability. In *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering-Software Engineering for AI* (pp. 100-111).

Xia, Z. (2023). Addressing the Tasks and Opportunities of Agency Using AI-based Chatbots. *International Journal of Communication Networks and Information Security, 15*(1), 25-42. https://www.proquest.com/scholarly-journals/addressing-tasks-opportunities-agency-using-ai/docview/2812106430/se-2

Yablonsky, S. (2021). AI-driven platform enterprise maturity: from human led to machine governed. Annales Universitatis Mariae Curie-Skłodowska, Sectio K – *Politologia, 50*(10), 2753–2789. https://doi.org/10.1108/K-06-2020-0384

Zhang, P., & Kamel Boulos, M.N. (2023). Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet, 15*(9), 286. https://doi.org/10.3390/fi15090286