1) Background / Problem Statement
Blue Cross Blue Shield (BCBS) is a large health insurance organization that operates through a nationwide network of independently licensed companies, providing coverage across the United States.

BCBS operations include:
- Individual and family health insurance plans
- Employer-sponsored health plans
- Medicare and Medicaid programs
- Claims processing and benefits administration
- Customer service and care coordination support

Workforce:
- Thousands of employees across insurance operations, clinical review, IT, and administrative roles

Key systems used:
- Claims processing and billing systems
- Member portals for coverage details, claims, and messaging
- Provider networks and authorization systems
- Internal IT ticketing and support platforms
- Secure databases containing PHI and insurance records

BCBS serves a large and diverse member population. While the organization is known for broad coverage and extensive provider networks, leadership has identified growing challenges related to service delays, high inquiry volumes, and increasing operational complexity. These pressures raise concerns about maintaining efficiency, accuracy, and member trust as demand continues to grow.

2) Objective
The objective of this project is to help Blue Cross Blue Shield (BCBS) improve operational efficiency and information accessibility for both employees and members. By implementing a secure, role-based AI system, BCBS aims to provide faster access to insurance and medical information, reduce reliance on customer service for routine inquiries, and give users a centralized platform to access their authorized information when needed.

3) Proposed Solution (BCBS_AI)
To address this challenge, BCBS proposes the use of a secure, role-based AI system that can assist patients and employees by tracking patient medical history and answering insurance-related questions, while maintaining strict data privacy and security controls.

4)Business Pressure / Operational Challenge

In 2024, Blue Cross Blue Shield experienced significant financial losses, demonstrating operational cost pressures. The company saw an increase of $3 billion for medical and pharmacy claims as well as losses ranging from $62 million to $1.7 billion across 7 of their plans. As of 2025, Blue Cross has begun offering voluntary separation packages with the aim to reduce costs and streamline operations.

- BCBS Michigan reported an operating loss of $1.7 billion and an operating margin of -4.2%.
- BCBS Massachusetts reported a net loss of $223.6 million and a -4.3% operating margin.
- Highmark Western and Northeastern New York reported a net loss of $140 million.
- Independence Health Group, the parent company of Independence Blue Cross, reported a net loss of $239 million in 2024.
- Arkansas BCBS reported a $226 million net loss.
- BCBS Rhode Island reported a net loss of $115 million.
- BCBS Vermont reported an underwriting loss of $62 million.

With these financial results and the failure to meet the 2025 financial plan, there has been increased pressure on leadership to control administrative costs and improve operational efficiency. In this case, AI is a good solution to reduce workload and increase productivity.

5)Where AI started showing Up (Informally)

Without a formal AI strategy or approved toolset, staff across the organization began using AI tools independently to assist with writing, summarization, and documentation. These practices emerged informally as employees attempted to manage increasing administrative workloads and operational pressure.

Insurance Provider

- Drafting and rewriting claim denial and approval explanations
- Drafting appeal responses and summarizing payer rules
- Converting clinical documentation into payer-friendly justifications

Doctors and Clinical Providers

- Drafting discharge instructions in plain language
- Rewriting clinical notes or care explanations for clarity
- Creating internal checklists for common follow-up or post-visit questions

IT and Administrative Staff

- Generating troubleshooting steps for recurring system issues
- Summarizing IT support tickets into internal knowledge base articles

- Drafting internal documentation and process guides

Patient

- Asking AI to interpret claim explanations, bills, or denial letters
- Summarizing visit notes or discharge instructions for personal understanding
- Drafting appeal letters or coverage questions before submitting them

While these uses improved efficiency and reduced individual workload, they were inconsistent, ungoverned, and largely invisible to leadership, introducing potential risks related to data privacy, accuracy, and regulatory compliance.

6) Trigger Events: Near-Miss Incidents

Incident One: Doctor

A doctor used an AI tool to draft documentation related to a patient's insurance claim. The AI output unintentionally included protected health information (PHI). This content was later reviewed by an insurance provider as part of the claims process, resulting in unnecessary exposure of sensitive patient data outside the appropriate clinical context. Although no data breach occurred, the incident highlighted the risk of PHI leakage when AI outputs are not properly reviewed or restricted by role.

Incident Two: Insurance Provider

An insurance provider used AI to revise and "clean up" a claim explanation. During this process, the AI modified numerical values associated with the claim. The error was not immediately identified, and the patient was incorrectly billed, resulting in the patient being charged significantly less than the correct amount. While the issue was later corrected, the incident demonstrated the financial and compliance risks of relying on AI-generated content without human verification.

Incident Three: IT Administrator

An IT administrator used AI to summarize system logs in order to speed up troubleshooting. The AI-generated summary omitted critical log details that were necessary to fully understand system behavior. As a result, the resolution of the issue was delayed. This incident exposed the risk of using AI for security or operational analysis without careful review of the original data.

Summary of Impact

Although none of these incidents resulted in long-term harm, they served as clear warning signs. Together, they demonstrated the need for formal AI governance at BCBS, including role-based access controls, prohibited inputs, required human review, and continuous monitoring.

7) Stakeholders and Their Priorities

Executive Leadership Team: Tasked with improving margins and operational efficiency while preserving brand trust with other stakeholders

- Margin recovery and cost control after 2024 losses across multiple BCBS plans

Policy & Legal Team: Ensure compliance with privacy and healthcare regulations during day to day operations as well as advancing initiatives

- Adherence to HIPAA to protect PHI with the use of AI in operations

IT & Security Team: Enhancing security and development of AI initiatives as well as maintaining existing technology. Reduce administrative burden as well as improve efficiency for providers and members

- Ensuring secure data exchange and preventing unauthorized data access

Operations Team: Reduce administrative burden, manage claims processing, provider portals, and improve service performance

- Use AI to automate documentation and assist with claims review while complying with the AI policy

Members & Consumers: Prioritize affordability, response times, transparency, and communication with providers

- Improvement in digital interactions and communication with the use of AI

8)Organizational Constraints

Financial Constraints: Multiple BCBS plans reported significant operating and underwriting losses, limiting available capital

Regulatory And Compliance Requirements: Must comply with HIPAA, state insurance regulations, CMS oversight, and evolving data privacy laws.

Structure Across Multiple Independent BCBS Plans: Governance must work across independently operated plans with different systems, vendors, and state requirements

Workforce Capacity: Cost-containment efforts and financial losses have led some BCBS plans to reduce headcount, increasing workload for remaining employees and limiting internal capacity to manage new initiatives

Brand Trust: Must protect member data and maintain public confidence by avoiding privacy breaches, compliance failures, or inconsistent communications

9) Decision Point

BCBS CEO requests a formal AI Use Policy within two weeks that:

- Allows AI use for productivity where it is safe and valuable
- Clearly defines approved tools and prohibited inputs (PHI, security data, incidents)
- Requires human review for patient-facing/clinical content
- Establishes a "help path" so staff can ask questions instead of guessing
- Includes examples that match real staff workflows patient portals, discharge instructions, appeals, IT tickets)
- Support AI as a managed organizational capability rather than an unmanaged operational risk

BCBS goal is to support AI as a managed capability not an unmanaged risk.

10)Definition of a Successful Outcome

- BCBS_AI provides consistent, accurate, and proficient assistance to all authorized staff members
- Employees across roles (insurance providers, doctors, IT/Admin) can efficiently complete tasks with AI support while staying within policy boundaries
- Patients receive clear, trustworthy, and easy-to-understand information about their insurance and care
- AI usage reduces workload and response times without compromising data privacy or security
- Human oversight ensures AI outputs remain accurate, compliant, and safe
- Increased trust in BCBS services due to secure and responsible AI use
- Improved customer satisfaction leads to stronger member retention and the attraction of new customers
- AI is recognized as a reliable, managed capability that enhances BCBS operations rather than introducing risk

https://www.beckerspayer.com/payer/6-bcbs-plans-reporting-losses-in-2024/
https://www.wral.com/news/state/blue-cross-nc-voluntary-separation-financial-challenges-october-2025/