AirGAP-AI

Offline, Privacy-First AI Technical Support Assistant

What is it?

AirGAP-AI is a fully offline AI assistant designed to provide technical support in privacy-sensitive environments such as healthcare, finance, and regulated enterprises. All processing occurs locally, and no data leaves the device.

The Problem

Organizations operating in regulated environments cannot safely rely on cloud-based AI tools. These tools introduce risks related to data exposure, compliance uncertainty, and dependency on external connectivity, while IT staff remain burdened by repetitive support requests.

The Solution

AirGAP-AI runs entirely on-device using a local language model and locally stored documentation. It provides useful technical guidance while intentionally refusing unsafe or non-compliant requests.

Key Design Principles

• Fully offline operation (air-gapped capable)
• No cloud services or external APIs
• No persistent chat history
• Strict refusal of patient data access
• No medical or clinical advice

What It Can and Cannot Do

Can: Explain software features, guide UI workflows, troubleshoot technical issues, and safely acknowledge unknowns.
Will Not: Access patient records, bypass access controls, interpret medical images, or provide diagnoses.

"In regulated environments, the safest AI is one that knows its limits."

Student: Harvansh Aneja
Capstone Project: AirGAP-AI

Project Summary: AirGAP-AI

Project Objective

This capstone project explores whether a useful AI technical support assistant can be deployed entirely offline while maintaining privacy, safety, and compliance-aligned behavior. The goal was to demonstrate feasibility rather than claim regulatory certification.

Motivation

Cloud-based AI systems introduce significant risks in regulated sectors, including data leakage, unclear retention policies, and reliance on continuous internet access. These risks motivated the design of a local-only alternative.

System Architecture

AirGAP-AI uses a locally deployed language model with retrieval-augmented generation (RAG) from locally stored documents. All inference occurs on-device, with no external communication or background logging to cloud services.

Safety and Compliance Approach

Rather than claiming HIPAA or GDPR compliance, the system demonstrates compliance-aligned behavior through refusal-by-design. Requests involving patient data, access control bypassing, or clinical interpretation are consistently refused.

Key Technical Features

- Offline local language model execution
- Document-based knowledge retrieval
- Prompt-enforced scope control and refusals
- Predictable and testable response behavior

Limitations and Future Work

The system is not a certified medical product and does not use real patient data. Future work includes role-based access control, encrypted audit logging, expanded datasets, and deeper UI integration.

Conclusion

AirGAP-AI demonstrates that privacy-first, offline AI systems can be both practical and responsible when constraints are treated as design features rather than limitations.