Patient note clinic web application (Demo Prototype)

1. SYSTEM OVERVIEW & OBJECTIVE

This project presents a secure, AI-assisted clinical note system designed for a single-patient workflow. The system focuses on:

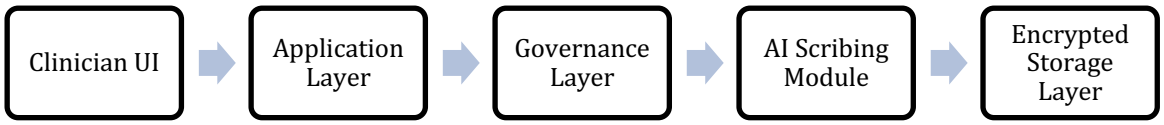
- Reducing clinician documentation burden
- Preserving traceability and data provenance
- Enforcing strict access control (RBAC)
- Preventing data leakage during AI-assisted writing

This is a demonstration prototype intended to show system design, governance thinking, and technical trade-offs rather than a production-scale deployment.

2. ARCHITECTURE OVERVIEW

The system follows a modular architecture with clear separation between user interaction, data governance, and AI-assisted logic.

High-level flow:



The Clinician interface is designed as a **single-patient page**, focusing on streamlined access to patient information. At the **application layer**, the system manages entries, supports commenting and highlighting of important information, and tracks version history for auditability.

1. The **governance layer** ensures privacy and compliance by applying a redaction engine to remove sensitive information, enforcing role-based access control (RBAC) to restrict visibility according to user roles, and maintaining provenance tracking to clearly link every note or highlight back to its source.

2. The **AI scribing module** operates exclusively on redacted context, generating draft notes that summarize recent consultations or patient interactions while preserving privacy.

3. Finally, all data is stored securely in the **encrypted storage layer**, with TLS protecting data in transit and encryption ensuring data at rest remains secure.

Key design principle:
AI never directly accesses raw sensitive data without redaction.

3. DATA MODEL & RELATIONSHIPS

All data entities are linked to a single patient page.

Core entities:
All data entities in this prototype are linked to a single patient page. The core entities include:

Entry: Represents a clinician-authored note or update and serves as the primary anchor entity.

Comment: Attached to a specific Entry, Comments are used for clarification, peer review, or task-related discussion.

Version: Each Entry can have multiple Versions, which are snapshots taken at specific points in time. This enables auditability and allows rollback to previous states.

Highlight: Highlights mark specific text spans within an Entry, serving purposes such as drawing attention, tagging critical information, or selecting context for AI processing.

Provenance: This metadata layer records the author, timestamp, role, and source of each change, ensuring traceability and trust in the system.

AI_Scribed_Notes: AI-generated draft outputs that are always linked to a specific Entry and Version. These notes assist clinicians while maintaining a clear lineage to the original content.

Relationship structure (simplified):

```
Entry
 ├── Versions
 │    ├── Highlights
 │    └── Provenance
 ├── Comments
 └── AI_Scribed_Notes
```

4. SECURITY, REDACTION & RBAC

Security is enforced by design rather than by policy alone.

Encryption:

All data transmitted over the network is protected using TLS. Additionally, all persisted data is stored in encrypted form to ensure confidentiality at rest.

Redaction:

Sensitive fields, such as patient identifiers, contact information, and other PHI, are stripped or masked before any AI access. Redaction occurs at the governance layer, ensuring that raw data never leaves the secure boundary.

RBAC (Role-Based Access Control):

The system defines distinct roles, including clinician, staff, patient, and admin. Permissions are strictly enforced both at the API level and within the data-access layer. Any AI processing operates under the lowest-privilege role, preventing unintended access or modification of sensitive data.

5. AI INTEGRATION & LEARNING SCOPE

The AI component functions as an assistive drafting tool.

Key constraints:
The AI component functions strictly as an assistive drafting tool. It does not make autonomous decisions and does not have direct write access to authoritative patient records. All outputs produced by the AI require human review and approval before being incorporated into the timeline.

Learning mechanism:
Regarding the learning mechanism, no online learning is performed on live patient data. For the purposes of the demo, the AI operates in a stateless inference mode only, which prevents unintended memorization of sensitive information.

6. ASSUMPTIONS & FIRST-PRINCIPLES THINKING

Key assumptions:
Key assumptions for this prototype include the use of a single-patient page, which simplifies navigation and access control. Clinicians require transparency over all AI outputs, and auditability of actions is prioritized over automation speed.

First-principles approach:
From a first-principles perspective, every AI action must be explainable, every text change must be fully traceable, and governance is considered an integral part of the system architecture rather than an optional add-on.

7. TRADE-OFFS & SCOPE DECISIONS

Deliberate trade-offs:
The prototype makes deliberate trade-offs to balance functionality and safety. Automation is intentionally reduced to minimize risk, learning capabilities are limited to prevent unintended data leakage, and the clinical scope is narrowed to ensure clarity of design.

Out of scope:
Out of scope for this prototype are multi-patient dashboards, cross-institution data sharing, and real-time AI retraining.

8. CONCLUSION
This system demonstrates how AI-assisted clinical documentation can be designed with security, governance, and human oversight as first-class concerns.

The prototype prioritizes trust, traceability, and compliance over raw AI capability, reflecting real-world healthcare needs.