Assignment 1: HIPAA-Compliant Medical Report Explanation Flow

1. Short-Answer Questions:

- Preventing PHI Leakage:
  - Use TLS for data in transit and AES-256 encryption at rest.
  - Apply strict RBAC (Role-Based Access Control).
  - Anonymize or redact PHI during LLM prompt handling.
  - Ensure proper logging and monitoring.
- Two Required Audit Log Events:
  - Access logs: Who accessed PHI and when.
  - Data transmission logs: When PHI was sent, to whom, and by what method.
- Detecting and Remediating Hallucinations:
  - Implement confidence scoring and human-in-the-loop review.
  - Use NER (Named Entity Recognition) to detect unexpected terms.
  - Include fact-checking layer to validate medical facts before user sees them.
- Ensuring Only Right Users See Reports:
  - Enforce user authentication (e.g., OAuth2, biometrics).
  - Provide access tokens with expiration.
  - Display reports only over secure sessions, require re-authentication for access.

2. Sample Prompt:

- Sample Prompt:

"Given this CBC report, explain in simple, patient-friendly language the key results, avoiding any PHI or personal details. Highlight abnormal values and what they may indicate medically. Do not diagnose or prescribe."

- Evaluation of Compliance:
  - Ensure no PHI (name, DOB, patient ID, etc.) is present in the AI output.
  - Medical interpretations are consistent with clinical guidelines.
  - Log all AI outputs and have optional human review.

3. Outline:

- Explicit Consent:
  - Use a consent form prior to upload with clear checkbox confirmation.
  - Log consent with timestamp and IP for audit trail.
- What the User Sees After Upload:

  - Confirmation message, summary of what will be processed.
  - Option to cancel or view PHI warnings.
  - Progress bar or ETA for summary.
- Key Considerations:
  - Frontend: Responsive UI, offline handling, secure sessions.
  - Backend: Secure storage, logging, audit compliance.
  - AI Layer: PHI-stripping, hallucination detection, medical validation layer.