a. HIPAA and GDPR Compliance

Data Anonymization:

Mask or anonymize patient data when it is no longer needed for diagnostic purposes.

Audit Trails:

Log all access and changes to patient data with timestamps and user IDs.

Store audit logs securely for at least 6 years (as per HIPAA guidelines).

Training and Awareness:

Ensure all developers and operators handling the swarm are trained on HIPAA and GDPR regulations.

5. Agent Communication Protocol

Secure Inter-Agent Communication:

Encrypt messages between agents using shared secrets or public/private key pairs.

Communication Verification:

Add integrity checks (e.g., HMAC) to ensure messages between agents havent been tampered with.

- Structured outputs
- List of possible ICD 10 codes with supporting evidences, final_summary icd 10,

- icd 10
  - supporting evidence

- icd 10
  - supporting evidence
- icd 10
  - supporting evidence
- icd 10
  - supporting evidence
- most_likely_code:
  - code:
  - summary

- patient may have many conditions,
- patient needs to identify list of icd 10s, for every code, what is the servicing provider, what is evidence for that code including reference to page number,
- for every patient, generate unique id,
- for every doc in the database, attach some unique id, when we query the data using that id,
- same patient can be handled differently, document from different year'
- for some docs, average doc size is 20+ pages, but others is 300+, biggest document is 30,000 pages, overview of the entire patient and medical history of the patient
- handle the number of pages
- turn around time, handle processes of 100+ pages, process 30,000 pages