Q1)

- **Patient Safety is Critical**
    - Errors can cause injury or death.
- **Regulatory Compliance is Mandatory**
    - Must comply with strict regulatory frameworks before market release.
- **Extensive Documentation and Traceability**
    - Every requirement must link to design, code, tests, and risk controls.
- **Strict Change Management**
    - Even minor updates require impact analysis and re-validation.
- **Verification and Validation Beyond Testing**
    - Must prove clinical effectiveness, not just functional correctness.
- **Real-Time and Hardware Constraints**
    - Software interacts directly with sensors and actuators.
- **Cybersecurity as a Safety Requirement**
    - Security breaches can lead to patient harm.

  Usability as a Safety Factor
    - Poor interface design can cause clinical errors.
- **Long Product Lifecycles**
    - Devices remain in use for 10–15 years.
- **Legal and Liability Exposure**
    - Software defects may result in lawsuits and recalls.

Q2)

Patient Safety

- Prevents injury or death from software errors.
- Required by standards like ISO 14971 and IEC 62304.
- Forces:
    - Hazard analysis before coding
    - Safety-based requirements
    - Strict verification and validation
    - Full traceability
    - Controlled change management

Data Privacy (HIPAA, GDPR)

- **Protects Protected Health Information (PHI) from unauthorized access, misuse, or breaches.**
- **PHI = any identifiable health data (name, ID, diagnosis, ECG, lab results, device IDs linked to a patient).**
- **Legally enforced by:**
    - **Health Insurance Portability and Accountability Act (US)**
    - **General Data Protection Regulation (EU)**
- **Forces:**
    - **Encryption of PHI (data at rest and in transit)**
    - **Role-based access control to PHI**
    - **Audit logging of all PHI access**
    - **Data minimization (store only necessary PHI)**
    - **Breach detection and response procedures**
    - **Patient rights (access, correction, deletion under GDPR**

Q3)

Regulatory Bodies

- **U.S. Food and Drug Administration (FDA)**
    - Regulates medical devices in the United States.
    - Reviews safety and effectiveness before market approval.
    - Requires compliance with Quality System Regulation (21 CFR 820).
    - May require premarket submissions (510(k), De Novo, PMA).
- **CE marking**
    - Required to sell medical devices in the European Union.
    - Demonstrates conformity with EU MDR.
    - Involves conformity assessment via Notified Bodies (for higher-risk devices).

Significance of IEC 62304

- **IEC 62304**
    - International standard for medical device software lifecycle.
    - Defines required processes for:
        - Software development
        - Maintenance
        - Risk management integration
        - Problem resolution
    - Introducing software safety classes (A, B, C).
    - Mandatory or expected by FDA and EU regulators.

Q4)

Root Causes:

- Ambiguous requirements for unit handling and conversion (mg vs µg not strictly defined).
- Faulty business logic with no centralized unit control between EHR and pharmacy modules.
- Inadequate integration testing and absence of dosage range safety validation.

Solutions:

- Define strict unit standardization requirements with full traceability.
- Implement centralized conversion service with strong typing and hard-stop alerts for abnormal doses.
- Apply formal risk management and verification processes aligned with IEC 62304.

Q5)

- **Regulatory Focus:** Clinical systems (EHR/PACS) follow HIPAA, GDPR; medical device software follows FDA, IEC 62304, ISO 14971.
- **Safety Criticality:** Embedded device software is often life-critical; EHR/PACS failures affect workflow/data but rarely cause immediate harm.
- **Development Lifecycle:** Device software uses strict V-model or risk-based iterative processes; EHR/PACS can use agile or iterative models.
- **Testing & Validation:** Device software requires exhaustive unit, integration, and verification with traceability; EHR/PACS emphasizes functional, usability, and security testing.
- **Deployment & Updates:** Embedded devices have controlled, infrequent updates; clinical software supports continuous updates, patches, and scalability.
- **Hardware Dependency:** Embedded software tightly coupled with device hardware; EHR/PACS mostly hardware-agnostic, cloud or server-based.

Q6) d) User Interface Color Schemes

Q7) F

Q8) c) Protected Health Information

Q9) F

Q10) DICOM