1. Establishment of PCC Enterprise Data Center

1.1 Data Center Facility Setup

Build a **Tier II or Tier III–aligned** data center (depending on budget of PCC):

- Raised flooring or optimized hot/cold aisle layout
- Environmental control: precision AC, humidity control, leak detection
- UPS (N+1), PDU systems, and generator integration
- Fire suppression system (FM200 or Novec 1230)
- Access control + CCTV monitoring
- Redundant power and network routing
- Secure equipment rack/cabinet configuration

1.2 Core Compute and Virtualization Platform

Deploy an enterprise-grade server infrastructure with virtualization for flexibility.

- **Compute nodes** (3–6 servers minimum)
- **Virtualization platform:** VMware
- High-density CPU and RAM configuration
- GPU-enabled servers for:
    - Clinical imaging
    - AI-driven diagnostics
    - Analytics

This environment will host:

- Hospital Information System related to Cancer Patients from various hospitals (central repository)

1.3 Enterprise Storage System

Install fault-tolerant, scalable storage architecture:

- **SAN/NAS unified storage**
- Minimum **200TB**
- SSD tier for databases and HIS
- HDD tier for PACS images and archives
- A separate **warm archive** for older data
- Support for:
    - RAID 6 / RAID 10
    - Snapshots
    - Replication
    - Deduplication
    - Compression

---

2. PACS, RIS, LIS, EMR & Digital Health Systems Integration

2.1 Clinical Information Systems Deployment (still don't know if possible ba na magkaroon kami nito)

The data center will host and integrate:

- **HIS / EMR**
- **PACS** (Radiology imaging)
- **RIS** (Radiology workflow)
- **LIS** (Laboratory diagnostics)
- **Pharmacy Information System**
- **Oncology Information Management Suite**
- **Telemedicine platform**

2.2 Interoperability & Data Exchange

- Adopt **HL7, FHIR, DICOM, IHE profiles**

- Establish an **Integration Engine** (Mirth/NextGen, Rhapsody, InterSystems HealthConnect)
- Build a **Health Information Exchange (HIE)–ready architecture**
- Integration with DOH central reporting modules
- Registries for:
    - Cancer patients
    - Radiology studies
    - Laboratory results
    - Medication and chemotherapy cycles

---

3. Network & Security Enhancements for Hospital Operations

3.1 Network Modernization

- Full hospital-wide network refresh
- Segmented VLANs for clinical, admin, guest, biomedical devices
- 10G uplinks across core–distribution–access layers
- Redundant network routing and switching
- Enhanced wireless coverage for all clinical floors

3.2 Enhanced Cybersecurity Stack

- Next-generation firewall (XGS 4300 HA) integration with DC
- Endpoint detection & response (EDR) for all clinical workstations
- Zero Trust Network Access (ZTNA) rollout
- Data Loss Prevention (DLP) for patient records
- SIEM (Security Information and Event Management) deployment
- Regular vulnerability scanning and penetration testing

---

4. Data Management & Resilience

4.1 Backup and Disaster Recovery Strategy

Implement multi-layered backup:

- Primary onsite backup storage
- Secondary offsite DR backup (cloud or another DOH facility)
- Daily incremental, weekly full backups
- Automated replication of mission-critical systems

4.2 Business Continuity Planning

- Failover procedures
- Emergency operations center readiness
- Clear RTO/RPO definitions (Example: PACS RTO < 30 minutes)
- Periodic DR drills

---

5. Smart Hospital & Digital Innovation Roadmap

Phase 2 prepares PCC for modern innovations:

- AI-assisted imaging diagnostics
- Analytics and big data for cancer statistics
- IoT-enabled medical devices (ICU, monitoring systems)
- Smart nurse call and patient tracking systems
- Digital signage and wayfinding
- Telemedicine and remote oncology consultations
- Patient portal + mobile app integration

(Architectural)

1. Smart Access Control System (Hospital-Wide)

1.1 Multi-Layer Access Control

Different authentication levels depending on room criticality:

Level 1 – General Staff Areas

- RFID hospital ID cards
- PIN code fallback
- Timekeeping integration (bio-attendance)

Level 2 – Sensitive Clinical Areas

- Dual authentication: **RFID + Fingerprint**
- For areas like:
  - Laboratories
  - Radiology

Level 3 – High Security Zones

- **Facial recognition / vein recognition** for:
  - ICU
  - NICU / PICU (if applicable)
  - Medicine storage
  - Cashier vault room
- Anti-passback rules (prevents tailgating)

Level 4 – Data Center and Server Rooms

- **Retina/iris scanner + RFID + PIN combo**
- 3-factor authentication
- Strict access log and audit trail
- Mantrap doors (two-door interlock system)

- Integration with CCTV for identity validation

---

2. Biometric Technologies to Be Deployed

2.1 Fingerprint Biometrics

- For normal staff identification
- Fast, cheap, reliable

2.2 Facial Recognition

- For clinical areas
- Mask-tolerant models (hospital-ready)
- Used for:
    - Staff
    - Visitors (optional visitor management kiosk)

2.3 Palm Vein / Finger Vein Scanners

- More accurate than fingerprint
- Works even when gloves or alcohol are used
- Ideal for:
    - Operating theaters
    - Oncology drug preparation
    - Pharmacy vault

2.4 Retina / Iris Scanners

- Highest level of security
- Only used for:
    - Data center
    - High-security research areas
    - Medical records core storage
- Non-contact for hygiene compliance

3. Smart Door and Locking Systems

3.1 Electronic Door Locks (Maglocks / Door Strikes)

- All critical areas with automatic fail-safe/fail-secure modes
- Door monitoring: open/close, forced entry, tailgating detection

3.2 Mantrap Rooms

Installed in:

- Data Center
- IT Core Room
- Medicine vaults

Purpose:

- One person at a time
- Biometric validation needed to exit and enter
- Prevent piggybacking and unauthorized staff entry

3.3 Panic Buttons & Emergency Bypass

- Installed in clinical areas
- Integrated with fire detection and automated unlocking during emergencies

4. CCTV & Surveillance Integration

4.1 AI-Powered CCTV System

- 4K IP cameras with:
  - Facial capture
  - Object tracking
  - Motion detection
  - License plate recognition
  - Automatic incident detection (fights, falls, loitering)

4.2 Coverage Areas

- All entrances/exits
- Hallways
- Laboratories
- Data center (inside and outside)
- Power room and genset area

4.3 Central Monitoring

- Security command center in the Data Center control room
- 24/7 monitoring with redundant NVR storage

---

5. Visitor & Contractor Management System

5.1 Smart Kiosk Registration

- Self-check-in kiosks
- QR code visitor badge
- Destination-based access rules
- Health declaration integration (optional)

5.2 Temporary Access Control

- Time-limited QR or RFID
- Tracking of all visitor movement
- Contractor access scheduling with logs

---

6. Asset & Equipment Security

6.1 RFID Asset Tracking

- High-value equipment tagged:
  - Infusion pumps
  - Monitors

    - Portable ultrasound
    - Laptops
    - Medication carts

6.2 Exit Gate Scanners

- Automatic alarm if tagged equipment leaves unauthorized exit

---

7. Data Center–Specific Physical Security

7.1 Layered Security Zones

1. **Outer Zone (Restricted Floor)** – RFID + CCTV
2. **Inner Zone (IT Corridor)** – RFID + PIN
3. **Core Zone (Data Center Mantrap)** – Retina/Iris + RFID
4. **Server Racks** – Biometric locking cabinets

7.2 Environmental Monitoring

- Temperature/humidity sensors
- Leak detection
- Fire suppression system (Novec 1230)
- Door alarms
- Motion sensors

7.3 Redundant Power & Network

- Dual UPS
- Dual power feeds to all racks
- Redundant fiber uplinks
- Access control connected to UPS for fail-safe operation

---

8. Smart Building Integrations

8.1 Unified Security Management Platform

All systems integrated into one console:

- Biometrics
- Access control
- CCTV
- Fire alarm
- Visitor management
- Data center environmental monitoring

8.2 Automated Alerts

- Unauthorized access attempt
- Door forced open
- Temperature spike
- Water leak
- Power outage
- Suspicious movement