Below is a **complete, healthcare-grade Security Architecture** for **Zero Trust Architecture (ZTA)** with **PII/PHI protection and HIPAA compliance**, written at **CISO / Principal Security Architect depth** and aligned with the enterprise, solution, data, and application architectures you already created.

This is **audit-ready, board-ready, and interview-ready**.

Security Architecture – Zero Trust, PII/PHI, HIPAA

Scope: Multi-product healthcare platform (clinical, member, provider, analytics, AI)
Threat model: External attackers, insider threats, ransomware, data leakage, AI misuse

---

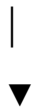
1️⃣ Security Architecture Principles (Non-Negotiable)

1. **Never trust, always verify**
2. **Assume breach**
3. **Least privilege everywhere**
4. **Identity is the new perimeter**
5. **Data-centric security over network-centric**
6. **Encrypt everything**
7. **Audit everything**
8. **Automate enforcement**
9. **Human-in-the-loop for clinical risk**
10. **Compliance by design, not by documentation**

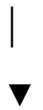
2️⃣ Zero Trust Reference Architecture (Logical)

User / System

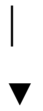
Identity Provider (IdP)



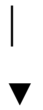
Policy Decision Point (PDP)



Policy Enforcement Point (PEP)



Application / Data / API / AI Service



Continuous Monitoring & Analytics

No implicit trust based on network location.

3️⃣ Identity & Access Management (IAM)

Identity Types

- Workforce (clinicians, staff)
- Members
- Partners
- Applications / services
- Devices

Controls

- OIDC / OAuth2
- MFA mandatory
- Conditional access (device, location, risk)
- RBAC + ABAC

- Privileged access management (PAM)
- Just-in-time access

4️⃣ Network Security (ZTA-aligned)

Controls

- Microsegmentation
- Private endpoints
- No flat networks
- East-west inspection
- Egress controls
- Service mesh mTLS

Outcome

Compromise of one service cannot spread laterally.

5️⃣ Application Security Architecture

Mandatory

- OAuth2 token validation
- Fine-grained authorization
- Input validation
- Output encoding
- Rate limiting
- API gateway enforcement
- Secrets from vault
- Secure headers
- Dependency scanning

6️⃣ Data Security Architecture (PII/PHI)

Classification

- Public
- Internal
- Confidential
- Restricted (PHI/PII)

Controls by level

Control	PHI/PII
Encryption at rest	Mandatory
Encryption in transit	Mandatory
Tokenization	Mandatory
Masking	Dynamic
Access logging	Mandatory
Retention rules	Enforced
Consent enforcement	Mandatory

7️⃣ PHI & HIPAA Controls Mapping

HIPAA Rule	Architecture Control
Access Control	IAM, RBAC/ABAC
Audit Controls	Immutable logs
Integrity	Hashing, versioning
Transmission Security	TLS, mTLS
Person/Entity Auth	MFA, IdP

HIPAA Rule	Architecture Control
Minimum Necessary	Data contracts
Breach Notification	SIEM + SOAR

8️⃣ Encryption & Key Management

- TLS 1.2+ everywhere
- AES-256 at rest
- HSM-backed KMS
- Key rotation
- Envelope encryption
- Separate keys per domain
- Bring-your-own-key (BYOK) support

9️⃣ Logging, Monitoring & SIEM

Collected

- Auth events
- Data access
- API calls
- Admin actions
- Model access
- GenAI prompts

Sent to

- Central SIEM
- UEBA
- SOAR for automated response

Logs are immutable and retained per policy.

🔟 Threat Detection & Response

Capabilities

- UEBA
- EDR/XDR
- Anomaly detection
- Ransomware detection
- Insider threat detection
- Automated isolation
- Forensics

1️⃣1️⃣ DevSecOps Security Architecture

Shift-left controls

- SAST
- DAST
- SCA
- IaC scanning
- Secret scanning
- Image scanning
- Policy as code

No scan = no deploy

1️⃣2️⃣ Data Platform Security (Analytics, ML, GenAI)

Controls

- Domain isolation
- Row/column-level security
- Secure views
- Data clean rooms
- Feature store access controls
- Model registry RBAC

1️⃣3️⃣ GenAI Security Architecture (Critical)

User

↓

AI Gateway

↓

Policy Engine

↓

Prompt Guardrails

↓

RAG (Governed Sources)

↓

LLM

↓

Output Validation

↓

Audit Log

↓

Human Review (if needed)

Guardrails

- No PHI to public LLMs
- Prompt injection detection
- Output hallucination detection
- Prompt versioning
- Model access control
- Human approval for clinical use

1️⃣4️⃣ Third-Party & Vendor Security

- Business Associate Agreements (BAA)
- Vendor risk assessment
- Token-based access
- No shared credentials
- Continuous monitoring
- Data minimization

1️⃣5️⃣ Backup, DR & Ransomware Protection

- Immutable backups
- Offline copies
- Automated restore testing
- Segregated admin access
- Rapid isolation
- Incident playbooks

1️⃣6️⃣ Governance, Risk & Compliance (GRC)

Evidence generated automatically

- Access reviews
- Audit logs
- Scan results
- Change records
- Policy enforcement logs

Auditors read systems, not documents

1️⃣7️⃣ Security Architecture KPIs

- PHI access violations (0)
- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- % encrypted traffic (100%)
- Privileged access age
- Audit findings (0 critical)

1️⃣8️⃣ Common Failure Modes & Mitigations

Failure	Mitigation
Flat network	Microsegmentation
Shared credentials	IAM + PAM
PHI leakage	DLP + masking
Overprivileged access	JIT + ABAC
AI hallucinations	RAG + validation
Audit gaps	Immutable logs

1️⃣9️⃣ Why This Security Architecture Works

- Enforces **Zero Trust end-to-end**
- Protects **PII/PHI by design**
- Supports **HIPAA audits automatically**
- Works with **multi-product scale**
- Enables **safe analytics & AI**
- Reduces blast radius
- Is automation-first

🎯 Executive one-liner (use this)

“This security architecture enforces Zero Trust and HIPAA compliance by making identity, data, and audit controls mandatory at every layer — so security is automatic, not optional.”
