01 / ILLUSTRATIVE ARCHITECTURE

Hospital-owned AI

Patient data stays within the institution. A proposed local predictive analytics design.

> Hypothetical design, not an SMCPA client engagement or a deployed system. No patient data or live predictions are processed on this website. No results, certifications or HIPAA compliance are claimed. This is not a completed engagement or a compliance guarantee.

A hypothetical hospital wants to analyze its own patient records to estimate readmission risk and forecast bed demand. SMCPA could help define the business case, governance, financial model and delivery roadmap, working with the hospital's qualified engineers, clinicians, privacy officer and legal counsel to build and sustain a local system.

Hospital-controlled environment

1. **Patient records**
   Approved EHR extracts; data purpose, quality and access verified.
2. **Protected data layer**
   Locally stored, access-restricted data with traceable transformations.
3. **Local prediction model**
   Training and inference on hospital-managed compute; no external model calls.
4. **Care-team review**
   Authorized clinicians review risk estimates inside the hospital workflow.

In this proposed design, ingestion, storage, model training, inference, logs and backups remain within hospital-managed infrastructure. External model APIs, telemetry and PHI exports are disabled. Vendor maintenance, if needed, uses institution-approved access within that boundary.

02 / SAFEGUARDS

Privacy, security & oversight

Safeguards to assess, implement and sustain—not a certification checklist.

> Keeping data on-site is not enough to establish HIPAA compliance. The hospital must assess the actual uses, safeguards, contracts and applicable laws with privacy and legal professionals. Compliance depends on implementation and ongoing operations, not the location of a server.

01 Approved purpose & data use

Document the permitted basis for treatment or healthcare operations. Research and secondary uses require separate review. Apply minimum-necessary standards where applicable; treatment disclosures have exceptions.

02 Risk analysis & safeguards

Conduct and document security risk analysis and risk management; implement appropriate administrative, physical and technical safeguards, including access controls, authentication, audit controls and transmission protections.

03 Hospital-controlled access

Use role-based access, least privilege, institution-managed identities and reviewed access logs. Encrypt data at rest and in transit as a design safeguard, manage keys locally and document retention and recovery procedures.

04 Vendor & contract controls

If SMCPA or another vendor creates, receives, maintains or transmits PHI as a business associate, execute an appropriate BAA before access and address subcontractors. On-site work does not remove this requirement.

05 Clinical validation & oversight

Validate on local data before use, review bias and performance across patient groups and monitor drift. Clinicians retain decision authority; the model must not autonomously diagnose, treat or deny care. Review any applicable FDA and other requirements.

06 Sustained institutional ownership

The hospital owns operational approvals, security monitoring and incident response. Maintain versioned models, change approval, restore tests, workforce training and a documented rollback process.

03 / DELIVERY & EVALUATION

From feasibility to pilot

Illustrative 16-week planning schedule, not a delivery promise. Governance, data quality, validation and approvals determine whether the project proceeds.

Weeks 1–3	**Scope & approval** Confirm the use case, legal basis, data inventory and business objectives.
Weeks 4–7	**Secure foundation** Establish local infrastructure, safeguards and documented access controls.
Weeks 8–12	**Build & validate** Develop with qualified teams; test locally and evaluate calibration, bias and reliability.
Weeks 13–16	**Controlled pilot** Run in shadow mode first; require approvals before clinical use and define monitoring and rollback.

Measure evidence—not promises

- Model discrimination and calibration on held-out local data
- Sensitivity, false alerts and performance by patient subgroup
- Care-team workload and workflow usefulness
- Readmission outcomes and cost impact only after a controlled evaluation

> No accuracy, savings or reduction in readmissions is assumed. These are evaluation measures, not projected results.

04 / REFERENCES & NEXT STEPS

Ground the design in evidence

Public guidance referenced by the website case study. Applicability requires institution-specific professional review.

1. HHS · Security Rule safeguards

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

2. HHS · security risk analysis

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

3. HHS · minimum necessary and exceptions

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

4. HHS · software vendors and BAAs

https://www.hhs.gov/hipaa/for-professionals/faq/256/is-software-vendor-business-associate/index.html

5. FDA · clinical decision-support guidance

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software

> This document is an illustrative proposal, not evidence of a completed SMCPA engagement, a deployed system, proven outcomes or a compliance guarantee. It is not legal or clinical advice. Hospital privacy, legal, security and clinical leaders must approve the actual design and operations.

Discuss your institution's AI readiness

SMCPA could support the business case, governance, financial model and delivery roadmap alongside qualified hospital technical, clinical, privacy and legal teams.

(713) 527-2343 | Info@SMCPA.Co

Read the Healthcare case study online