A PRACTICAL GUIDE FOR HEALTHCARE LEADERS

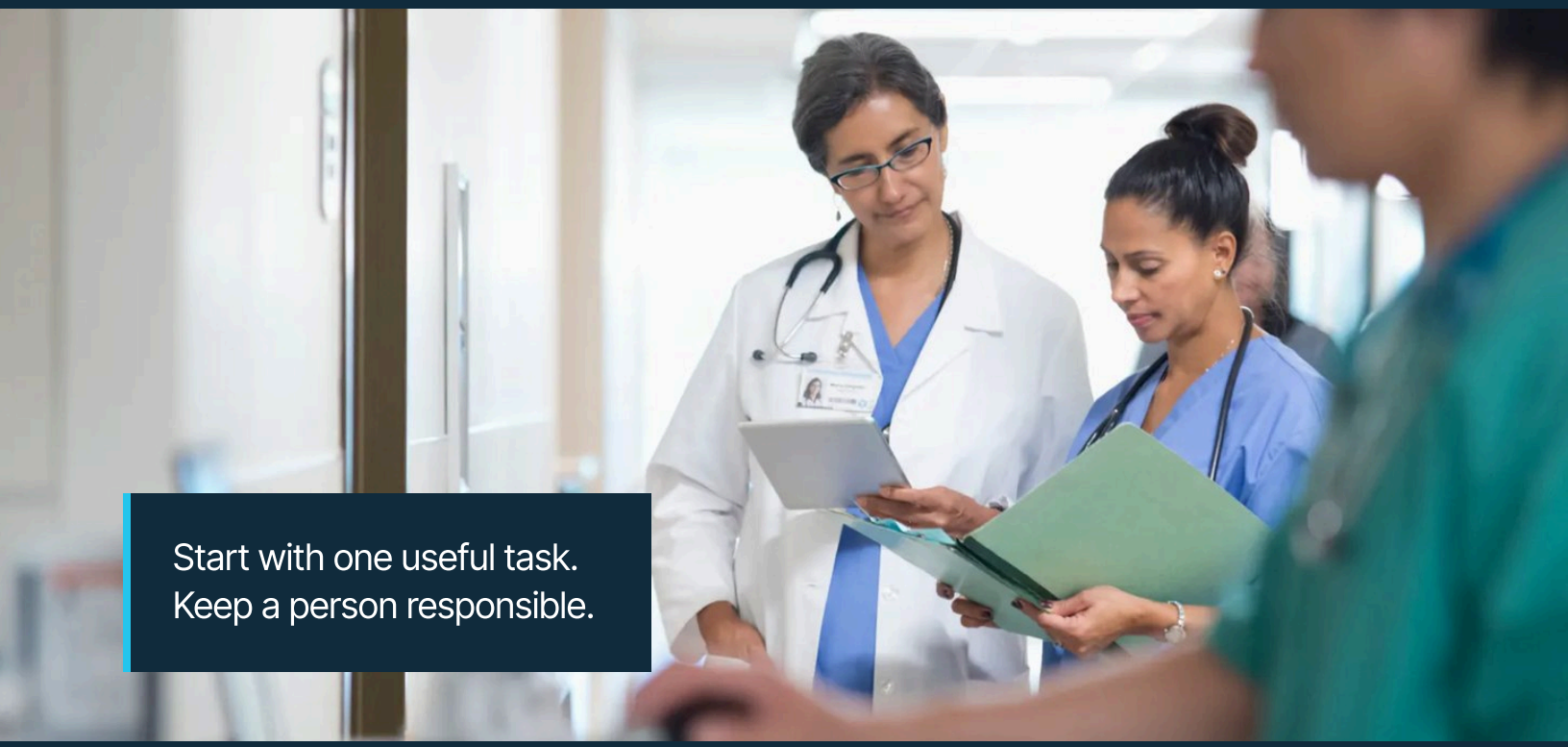
The Practical AI Implementation Guide for Healthcare

Protect patient information.
Support staff. Preserve clinical responsibility.

01 / Choose the workflow

02 / Protect the data

03 / Test and decide



> Start with one useful task.
> Keep a person responsible.

01 / START WITH THE WORKFLOW

A useful pilot starts with a clear boundary.

Reduce a specific burden while keeping patient safety, professional judgment and the existing care process in view.

01

Policy training

Turn a current, approved policy into a staff learning outline. The policy owner checks the result.

02

Patient education

Prepare a draft from approved public resources. Qualified staff review meaning and next steps.

03

Operations briefs

Summarize approved aggregate information. Keep proposals distinct from observed facts.

Begin with synthetic data.

Use approved nonpatient material until the workflow, contracts and controls are approved. Familiarity with a tool does not establish suitability for patient information.

OUTSIDE THIS STARTER PILOT

Diagnosis, triage, prescribing, treatment selection and other clinical decisions require a separate safety, regulatory and workflow assessment.

A clinician must be able to inspect and reject the output. Naming a reviewer is insufficient.

02 / WRITE THE PILOT CHARTER

Make the first decision before buying the tool.

A pilot charter makes allowed work, human review and stop conditions explicit.

Problem	Which repeated task creates delay, rework or avoidable burden?
Scope	Which staff, data, department and outputs are allowed?
Review	Who checks accuracy, safety and appropriateness?
Boundary	What may the tool never decide, send or change?
Stop	What event pauses the pilot, and who can act?

Observe the baseline

Watch representative tasks before introducing AI. Record total effort, corrections and handoffs. Compare similar work, not the fastest isolated demonstration.

Bring the right people

Include nursing, clinical leadership, privacy, security and the operational owner. Ask staff where errors and workarounds already occur.

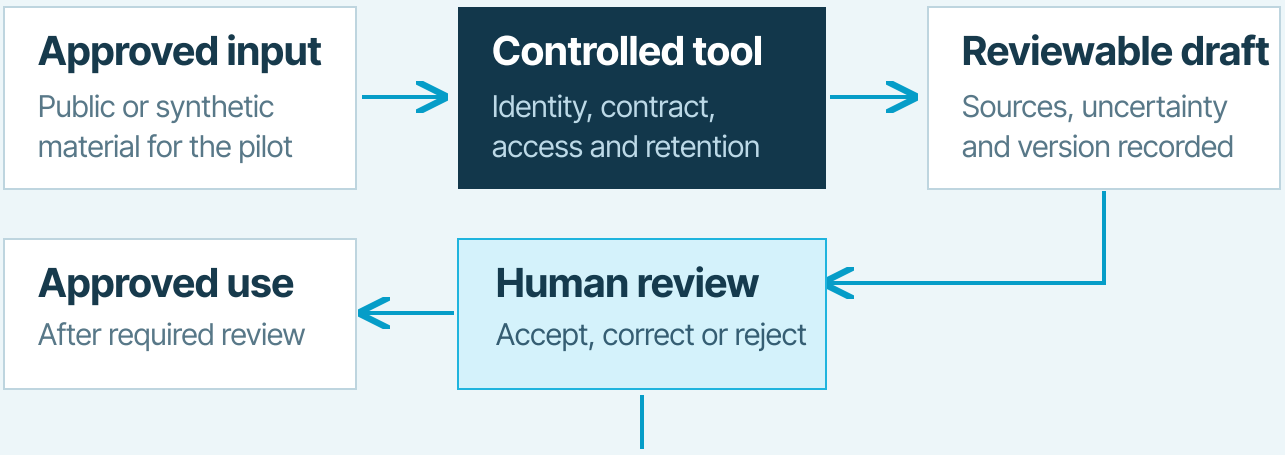
> **Example:** Compare the preparation and review time for a patient education draft using approved public material. Check that the final handout remains accurate and understandable.

03 / APPROVE THE DATA PATH

Follow the information. Then approve the workflow.

Approve every destination before using protected health information.

ILLUSTRATIVE DATA REVIEW MAP



Map beyond the prompt

Include source systems, recordings, generated text, integrations and every destination shown above. Minimize information at each step.

Approve the relationship

A cloud provider handling ePHI on a regulated entity's behalf can be a business associate even when it cannot decrypt the data. Determine the required agreement before use. [2]

> **Two checks that matter:** Removing names alone does not establish HIPAA de-identification. A business associate agreement does not replace risk analysis or controls. Use approved organizational review.

04 / ASSIGN THE CONTROLS

A deployment label is not a control plan.

Name each control owner. Verify the behavior in the actual workflow.

01 **Identity.** Unique accounts, role-appropriate access and prompt removal when no longer needed.

02 **Data use.** Enforce limits on training, secondary use, support access and disclosure.

03 **Retention.** Documented handling of prompts, recordings, outputs, backups and termination.

04 **Audit.** Protect evidence for investigation. Avoid unnecessary clinical content in logs.

05 **Recovery.** Tested continuity procedures and a practical way to disable the integration.

HOSTING CHOICE	QUESTIONS THAT STILL NEED ANSWERS
On-premises	Who patches, controls access, supports the system and tests recovery?
Cloud service	Are contracts, configuration and data responsibilities appropriate? [1, 2]

> **If information enters an unapproved service:** stop and contact privacy and security. Preserve evidence. Follow the incident process.

05 / PROMPT PATTERN: PATIENT EDUCATION

A draft for staff review. A source for every section.

Use approved public resources. Preserve clinical meaning.

COPY AND ADAPT / APPROVED NONPATIENT MATERIAL

> Using only these approved patient education materials, draft a plain-language explanation of [topic] for staff review. Preserve the source's warnings and instructions. Include questions the reader could ask their care team. Do not add a diagnosis, recommend a treatment, change a medication instruction or invent a citation. List unclear passages and identify the source for each section.

The reviewer checks the meaning.

- ✓ Meaning, warnings and instructions match the approved source.
- ✓ Reading level, accessibility and contacts fit the intended audience.
- ✓ Translations follow the organization's language-assistance process.

Keep the send step under human control.

Do not send generated material directly to a patient without the required review.

06 / PROMPT PATTERNS: STAFF AND OPERATIONS

Give the assistant a bounded assignment.

Use current approved sources. Expose gaps and uncertainty.

STAFF POLICY TRAINING

Teach the policy. Do not rewrite it.

> "Turn this approved policy dated [date] into a ten-minute staff training outline. Include the stated process, responsible roles, escalation contact and five knowledge-check questions with source references. Distinguish the policy's requirements from suggested teaching examples. Flag missing or conflicting instructions. Do not create a new policy."

Owner review: The policy owner validates the outline and answers. Resolve practice conflicts before training.

OPERATIONS BRIEFING

Separate observation from explanation.

> "Using these approved aggregate figures and nonpatient notes, prepare an operations briefing with observed issues, possible explanations, data limitations and questions for the team. Do not infer causation or individual performance. Label proposals as proposals."

Owner review: Check calculations independently. Small groups and detailed narratives can still expose individuals.

Writing authority is not action authority.

Keep scheduling, staffing, billing and record changes outside the assistant's authority unless separately assessed and explicitly approved.

07 / TEST BEFORE EXPANSION

Test the failure paths before the demonstration.

Use synthetic cases and approved source material. Define unacceptable results with the right specialists before testing.

Ordinary work	Does the output preserve meaning, cite the right source and respect the allowed task?
Missing or conflicting facts	Does the system identify unsupported answers and route uncertainty to a person?
Language and accessibility	Can the intended audience understand and use the output? Include relevant needs in the review set.
Access boundaries	Can an account retrieve another department's restricted information?
Logging and leakage	Does sensitive content appear in logs, support tools or other unintended destinations?
Hostile documents	Can instructions hidden in an uploaded document manipulate tool behavior or trigger unauthorized actions?

> **Test the whole workflow:** Record reproducible failures. Fix controls before repeating affected tests. Include the application, users and integration.

Risk organization: NIST AI RMF. Security scenarios: OWASP. Neither is certification. [4, 5]

08 / PRACTICE THE FALLBACK

Know how to stop. Know how to restart.

Staff need a working fallback while a concern is investigated.

1 **Disable and continue**

Disable the tool. Confirm staff can complete the underlying workflow without it.

2 **Withdraw and correct**

Withdraw or correct a flawed draft before it reaches patients or a clinical record.

3 **Revoke and verify**

Revoke a connector's credentials and verify the resulting access boundary.

4 **Investigate and authorize**

Record who investigates a safety concern and who approves restarting.

Clinical use needs its own assessment.

Qualified clinical and regulatory reviewers must evaluate intended use and actual function against FDA clinical decision support guidance. [3]

A generic assistant label or human review alone does not settle device status. Evaluate population, setting, evidence, foreseeable harm, training and failure response.

> Recheck material source, model, interface or integration changes. A cleared device or vendor study does not replace local assessment.

09 / MEASURE AND DECIDE

Count the whole task. Keep the evidence visible.

Compare similar work with the baseline. Include correction and support effort, and describe the limits of your sample.

Prepare	Review	Correct	Operate
Inputs and context	Accuracy and safety	Rework and gaps	Support and records

Measurement structure, not a forecast. Add licenses, infrastructure and support to total staff effort.

Quality	Reviewed examples, corrections and unresolved failure patterns.
Privacy and safety	Incidents, access findings and completed corrective actions.
Effort and cost	Total staff effort plus licenses, infrastructure and support.
Readiness	Owner, training, fallback, maintenance and review schedule.
Decision	Continue, narrow, change or stop. Record reasons and approver.

> **Expand one boundary at a time.** Patient information, a new department, a clinical function or write access requires a new assessment. Update training and documentation first.

Track inaccurate statements, missing warnings, unsupported references, access failures and workarounds. Faster drafting and staff satisfaction do not establish clinical benefit. Clinical outcome claims require appropriate evidence.

10 / PRIMARY SOURCES

Primary sources. Practical context.

Verify current requirements and guidance using these references.

01 **HHS HIPAA Security Rule summary**

Safeguards and risk analysis. Distinguish proposed changes from current requirements.

www.hhs.gov / Open the primary source

02 **HHS HIPAA and cloud computing**

Business associates, cloud responsibilities and risk analysis.

www.hhs.gov / Open the primary source

03 **FDA Clinical Decision Support Software guidance**

Function-specific review and non-device CDS criteria. Not blanket AI approval.

www.fda.gov / Open the primary source

04 **NIST AI Risk Management Framework**

Voluntary framework: Govern, Map, Measure and Manage. Not a certification.

www.nist.gov / Open the primary source

05 **OWASP Top 10 for LLM Applications**

Prompt injection, excessive agency and other application risks.

owasp.org / Open the primary source

> **Scope of this guide:** Planning support, not medical, legal or FDA regulatory advice. Qualified reviewers determine obligations and approval.

YOUR NEXT STEP

Bring one workflow. Leave with a clearer starting point.

A focused AI planning conversation starts with the task, the data and the people responsible for the result.

01 / THE WORKFLOW

The repeated task, its current burden and the staff who perform it.

02 / A SAFE EXAMPLE

A public or synthetic example that illustrates the task without patient information.

03 / THE DATA PATH

Where inputs, drafts, logs and connected services would go.

04 / THE DECISION

Your pilot criteria, review owner and the questions that remain open.

Plan Your Healthcare AI Pilot ↗

844-974-8669 · z7solutions.com

Keep patient information out of booking notes and initial examples.
Z7 Solutions LLC