Yes. Here is a simple, repeatable way to build a risk register from NIST SP 800‑66 Rev.2 and the NIST Risk Management Framework, in plain language and step by step. Think of it like a recipe any product can follow.

Overview of the idea

* Goal: List what could go wrong, how bad it would be, how likely it is, which safeguards apply, what will be done about it, and who owns fixing it, then keep it updated over time.
* Sources used: HIPAA Security Rule “what” (protect ePHI) and NIST guidance “how” (risk steps and control libraries).

Step‑by‑step process used

1. Define the scope in everyday words

* What system is being protected? For example: “AI clinical documentation tool with RAG, handling transcripts, embeddings, and draft notes that include ePHI.”
* Where does sensitive data live and move? List components: frontend, API, vector database, model, logs, storage, backups, vendor services.
* Why this matters: Without clear scope, risks will be missed or duplicated.

1. Write down what “bad things” could happen

* Brainstorm realistic “risk scenarios” in one line each: “PHI leaks through logs,” “model outputs unsafe advice,” “a staffer’s account is misused,” “vendor service mishandles data,” “system is down during clinic hours,” etc.
* Tip: Phrase each as cause → effect on patients/operations/compliance.

1. For each scenario, rate impact and likelihood

* Impact: How bad if it happens? High (endangers safety or serious HIPAA breach), Medium, or Low.
* Likelihood: How probable today? High, Medium, or Low.
* Inherent risk: The combo before any fixes (controls).
* Plain meaning: “Inherent” means the raw risk if nothing is done. “Residual” (later) is what’s left after fixes.

1. Attach the relevant HIPAA safeguards in plain terms

* HIPAA groups safeguards into Administrative (policies, training, vendor agreements), Physical (facilities, devices), and Technical (access control, encryption, audit, integrity, transmission security).
* For each risk, note which safeguard types obviously apply. Example: PHI leak → Technical (encryption, access, audit), Administrative (training, BAA).

1. Translate safeguards into concrete controls

* Use a common control language so teams know what to build and auditors recognize it. The widely used library is NIST “800‑53 controls” (short codes like AC‑2 for account management, SC‑28 for encryption at rest, AU‑12 for log generation).
* Pick the controls that match the risk. Example: PHI leak in logs → AC‑2/AC‑6 (least privilege), IA‑2 (MFA), SC‑13/SC‑28 (encryption), AU‑2/AU‑9 (log protection), SI‑10 (input validation).
* Plain meaning of a few codes:
  + AC = Access Control (who can do what).
  + IA = Identification & Authentication (prove who is who).
  + SC = System & Communications Protection (encryption, network).
  + AU = Audit & Accountability (logs, retention).
  + SI = System & Information Integrity (monitoring, validation).
  + IR = Incident Response (what to do when things go wrong).
  + CP = Contingency Planning (backups, disaster recovery).
  + SR = Supply Chain (vendors, provenance).

1. Record what exists vs. what is missing

* Existing controls: What is already in place (e.g., HTTPS, basic logging, role-based access).
* Gaps: What is missing (e.g., no MFA, logs may capture PHI, embeddings unencrypted).
* This comparison tells which fixes matter most.

1. Write a clear fix (mitigation plan) for each risk

* Be practical and testable. Example: “Turn on MFA for all staff,” “encrypt vector index at rest,” “scrub PHI before indexing,” “mask logs,” “clinician must sign off before note goes to EHR,” “add groundedness checks.”
* Add who owns it, a due date, and target “residual risk” (what level is acceptable after the fix).

1. Decide how to prove and monitor it

* Evidence: Screenshots, configs, policies, training logs, signed BAAs, test reports.
* Monitoring triggers: “Alert if PHI appears in logs,” “alert if groundedness <0.85,” “page on p95 latency >60s,” “monthly access review missed.”
* Residual risk: Re‑rate impact/likelihood after fixes; aim to move High to Medium or Low.

1. Keep it alive (not shelf‑ware)

* Review monthly/quarterly: close items, add new risks, update owners/dates, attach new evidence.
* Tie it to change management: When features change (e.g., new model, new vendor), add/update risks.
* Tie it to incident learning: After any incident, add its lessons to the register and playbooks.

Key jargon decoded

* ePHI: Electronic protected health information—person‑identifiable health data.
* Inherent risk: Risk before any controls.
* Residual risk: Risk after controls/mitigations.
* Control: A specific safeguard (policy, setting, technology, process).
* Baseline: A starting set of controls chosen for a system’s sensitivity.
* ATO (Authorization to Operate): Leadership’s formal acceptance that residual risk is tolerable; common in regulated environments.
* POA&M (Plan of Action & Milestones): The to‑do list of fixes with dates and owners.

How this connects to the frameworks, in simple terms

* HIPAA Security Rule says what must be protected and broadly how (administrative, physical, technical safeguards).
* NIST SP 800‑66 explains HIPAA in practical terms and gives activities and examples to implement those safeguards.
* NIST RMF is the stepwise process: Prepare (set roles/strategy), Categorize (decide how sensitive the system is), Select (choose controls), Implement (put them in), Assess (test), Authorize (leadership accepts residual risk), Monitor (keep watching).
* NIST 800‑53 is the control dictionary used to name the specific safeguards clearly.

Why this works for any product

* The steps are product‑agnostic: define scope, list bad things, rate them, map to safeguards, choose controls, fix gaps, prove and monitor.
* Swapping domains: For a different product (say, a claims adjudication API), repeat the same recipe but change the “where data lives,” the risk scenarios, and the control choices specific to that system’s architecture and vendors.

A quick mental checklist to reuse

* Scope? Users, data, systems, vendors.
* Risks? At least 8–12 realistic scenarios.
* Ratings? Impact, likelihood, inherent risk.
* Safeguards? Administrative, physical, technical.
* Controls? Name them with 800‑53 codes.
* Plan? Owner, date, steps, residual target.
* Proof? Evidence and alerts defined.
* Review? Regular cadence tied to changes/incidents.