Project Plan: Building a HIPAA-Compliant RAG Clinical Note Summarization Tool as an AI Product Manager

Key Takeaway:
By following this detailed, day-by-day roadmap—complete with deliverables, free open-source tools, and sample templates—you will both learn core AI product management practices in digital health and produce a shippable, HIPAA-compliant Retrieval-Augmented Generation (RAG) clinical note summarization prototype that showcases your PM skills.

Week 1: Foundations & Planning

Day 1: Define Vision, Scope & Stakeholders

- Task: Draft a one-page Product Vision document
  – Use this template: "Problem → Solution → KPIs → Users & Stakeholders."
  – Free sample: https://bit.ly/PM-Vision-Template
- Artifact: Product Vision (Google Docs link)
- Minute-level:
  09:00–10:00 AM: Research RAG basics (Hugging Face blog "RAG Explained")
  10:00–11:00 AM: Interview 1 stakeholder (e.g., a clinical scribe) via Calendly invite
  11:00–12:00 PM: Populate Vision template
  Afternoon: Share Vision draft for feedback in Slack channel

Day 2: Regulatory & Risk Assessment

- Task: Create HIPAA Compliance Checklist
  – Source: HHS.gov "HIPAA Privacy Rule" summary
  – Include: PHI de-identification, audit trails, encryption, BAAs
- Artifact: Compliance Checklist (Excel/Google Sheets)
- Minute-level:
  09:00–10:30: Read "HIPAA Privacy Rule" highlights on HHS.gov
  10:30–12:00: Draft checklist rows with "Requirement," "Owner," "Status"
  Afternoon: Map each requirement to product features (e.g., AES-256 encryption)

Day 3: User & Market Research

- Task: Conduct 3 user interviews and 1 competitor analysis
  – Tools: Otter.ai for transcription; Miro board for affinity mapping
- Artifact: User Interview Summary & Empathy Map
- Minute-level:
  09:00–11:00: Interview clinicians and scribes (30 min each)
  11:00–12:00: Transcribe via Otter.ai
  Afternoon: Affinity map insights in Miro; list 5 pain points

Day 4: Requirements & Prioritization

- Task: Write User Stories & prioritize via MoSCoW

```
– Format: “As a <role>, I want <feature> so that <benefit>.”
```

– Prioritize: Must/Should/Could/Won’t

- Artifact: User Story Backlog (Trello board)
- Minute-level:
  09:00–10:00: Draft 8 user stories (e.g., “As a clinician, I want automated note summary…”)
  10:00–11:00: MoSCoW prioritization workshop with mentor (Zoom)
  Afternoon: Populate Trello backlog and assign MoSCoW labels

Day 5: High-Level Architecture & Tech Stack

- Task: Draft System Architecture diagram
  – Components: Data ingestion, de-identification module, vector store (e.g., FAISS), RAG model, UI
  – Tools: draw.io (free)
- Artifact: Architecture Diagram (PNG export)
- Minute-level:
  09:00–10:00: Research MONAI clinical models on Hugging Face
  10:00–11:00: Sketch high-level flow in draw.io
  11:00–12:00: Annotate each component with open-source tool names
  Afternoon: Review with engineering lead via Loom video

Week 2: De-Identification & Data Pipeline

Day 6: Data Ingestion & Synthetic Data Setup

- Task: Source open MIMIC-III de-identified clinical notes
  – Register here: https://mimic.physionet.org/
  – Download sample notes CSV
- Artifact: Raw Data Folder & README

- Minute-level:
  09:00–10:00: MIMIC registration and access
  10:00–12:00: Download notes subset; store in Google Drive
  Afternoon: Write README.md explaining data schema

Day 7: PHI De-Identification Module

- Task: Implement de-identification using MIT's open-source deid library
  – Repo: https://github.com/mitre/deid
  – Output: CSV of sanitized notes
- Artifact: De-Identification Script & Demo Notebook
- Minute-level:
  09:00–10:00: Clone deid repo on local machine
  10:00–12:00: Configure JSON rules for names, dates, MRNs
  Afternoon: Run sample; validate no PHI remains

Day 8: Vectorization & Retrieval Setup

- Task: Load sanitized notes into FAISS vector store
  – Use sentence-transformers (Bio_ClinicalBERT)
- Artifact: Python script `index_notes.py` & sample index
- Minute-level:
  09:00–10:00: Install `faiss-cpu` and `sentence-transformers`
  10:00–12:00: Write code to embed and index notes
  Afternoon: Verify retrieval accuracy via example queries

Day 9: RAG Prototype Integration

- Task: Integrate Hugging Face RAG model with vector store
  – Model: `google/flan-t5-small` fine-tuned on clinical abstracts
- Artifact: Jupyter Notebook `rag_demo.ipynb`
- Minute-level:
  09:00–11:00: Load vector store and RAG model
  11:00–12:00: Build end-to-end pipeline: query → retrieve → generate summary
  Afternoon: Test on 5 sample cases; log summary quality

Day 10: Security Hardening & Encryption

- Task: Encrypt vector store and deploy local Key Vault simulation
  – Use HashiCorp Vault OSS
- Artifact: Deployment guide & config files
- Minute-level:
  09:00–10:00: Install Vault local dev server
  10:00–12:00: Script to encrypt/decrypt index files using Vault KMS
  Afternoon: Document security steps in Confluence page

Week 3: UI, Access Controls & Audit Trails

Day 11: UI Wireframes & UX

- Task: Create wireframes for clinician dashboard summarization UI
  – Tools: Figma free tier
- Artifact: Figma file with screens (Login, Upload, Summary view)
- Minute-level:
  09:00–10:00: Sketch on paper key screens
  10:00–12:00: Build in Figma; annotate with user actions
  Afternoon: Review with UX mentor on Loom

Day 12: Frontend Prototype (React)

- Task: Scaffold React app with three pages
  – Use Create React App (CRA) with Tailwind CSS
- Artifact: GitHub repo `rag-ui` with initial scaffold
- Minute-level:
  09:00–10:00: Run `npx create-react-app rag-ui`
  10:00–12:00: Install Tailwind per docs
  Afternoon: Create placeholder screens matching Figma

Day 13: Backend API & Access Controls

- Task: Build Flask API endpoints for summarization with JWT auth
  – Use PyJWT and role-based checks
- Artifact: Flask service code & Postman collection
- Minute-level:
  09:00–10:00: Initialize Flask project; install dependencies
  10:00–12:00: Implement `/login`, `/summarize` endpoints with role guard
  Afternoon: Test endpoints via Postman; export collection

Day 14: Audit Trail Logging

- Task: Implement immutable audit log using SQLite + git-backed logs
- Artifact: Logging module and sample logs
- Minute-level:
  09:00–10:00: Design audit schema (user, action, timestamp, note_id)
  10:00–12:00: Code logger to append and commit logs to private Git repo
  Afternoon: Validate log integrity by simulating unauthorized access

Day 15: End-to-End Stitch & Demo

- Task: Deploy full stack locally via Docker Compose
  – Components: Flask API, React UI, FAISS service, Vault
- Artifact: `docker-compose.yml`, README for launch
- Minute-level:
  09:00–12:00: Write Dockerfiles and Compose file
  Afternoon: Run `docker-compose up`; demo basic summarization

Week 4: Testing, Metrics & Launch Prep

Day 16: Functional & Usability Testing

- Task: Write test cases (pytest for backend; React Testing Library for UI)
- Artifact: Test suite and coverage report
- Minute-level:
  09:00–11:00: Backend unit tests for each endpoint
  11:00–12:00: UI snapshot tests for key components
  Afternoon: Achieve ≥80% coverage; document in Confluence

Day 17: Performance & Security Testing

- Task: Load test summarization API (Locust.io) and run OWASP ZAP scan
- Artifact: Test reports & remediation plan
- Minute-level:
  09:00–11:00: Define Locust scenarios (100 users, 1 RPS)
  11:00–12:00: Run Locust; record latency and failure rates
  Afternoon: Run ZAP; log vulnerabilities; propose fixes

Day 18: Define Success Metrics & Dashboard

- Task: Draft Analytics spec for metrics (e.g., summary latency, accuracy, usage)
  – Use Google Analytics free + custom events
- Artifact: Metrics dashboard mockup (Google Data Studio)
- Minute-level:
  09:00–10:00: List KPIs: Time saved, accuracy vs. gold standard, user adoption
  10:00–12:00: Build sample charts in Data Studio
  Afternoon: Share for stakeholder feedback

Day 19: Documentation & Training Materials

- Task: Create User Guide, API Docs (Swagger UI), and Admin Guide
- Artifact: Confluence space links; exported Swagger JSON
- Minute-level:
  09:00–11:00: Write step-by-step user manual with screenshots
  11:00–12:00: Annotate Swagger for each endpoint
  Afternoon: Draft Admin setup and maintenance guide

Day 20: Final Demo, Feedback & Roadmap

- Task: Present working prototype to mock stakeholders (via Zoom)
  – Gather feedback, log into Jira board as improvements
  – Draft next-phase Roadmap (v1.1 with EHR integration, QA enhancements)
- Artifact: Demo video link + Roadmap slide deck
- Minute-level:
  09:00–10:00: Prepare slide deck (Vision, Architecture, Demo, Metrics)
  10:00–11:00: Conduct demo; record session
  Afternoon: Update Jira with 10 backlog items; share Roadmap

Outcome & Showcased Artifacts:

- Vision doc, compliance checklist, user stories, architecture diagram
- Code repos (de-identification, RAG pipeline, UI & API)
- Wireframes, test suites, metrics dashboard
- Demo video & Roadmap deck

Following this plan demonstrates end-to-end product management skills—stakeholder engagement, regulatory planning, user research, backlog management, sprint execution, launch readiness—that position you as an outstanding Senior AI Product Manager candidate in digital health.

⁂

One-Week Shadow Plan: Delivering a Shippable HIPAA-Compliant RAG Clinical Note Summarization Tool

Key Takeaway:
In seven consecutive days—from stakeholder discovery through demo—you will shadow a senior AI Product Manager, learn on the go via curated free resources, and produce a working, HIPAA-compliant Retrieval-Augmented Generation (RAG) prototype complete with key artifacts.

Day 1: Foundations & Stakeholder Alignment

1. Morning (9:00–12:30) – Learn & Define

- Read "What Is Product Management?" by Product School (10 min): https://bit.ly/PS-IntroPM
- Study RAG fundamentals in the Hugging Face Tutorial (20 min): https://bit.ly/HF-RAG
- Draft a **One-Page Vision** using this simple template:
  - **Problem:** Clinicians spend excessive time on clinical documentation.
  - **Solution:** AI-powered summarization of notes via RAG.
  - **KPIs:** 40% reduction in documentation time; 95% summary accuracy.
  - **Users:** Clinicians, health scribes, compliance officers.
- **Artifact:** Google Doc "Vision & KPIs."

2. Afternoon (13:30–17:00) – Stakeholder Interviews & Research

- Learn basics of user interviews (15 min): https://bit.ly/NNG-Interview
- Conduct **2 short interviews** (30 min each) with clinicians or scribes:
  - Ask: "What slows your note-taking?" and "What summary format helps most?"
- Transcribe via Otter.ai (free tier).
- Create an **Empathy Map** in Miro (free): https://miro.com/templates/empathy-map/
- **Artifact:** Miro board "Empathy Map & Pain Points."

Day 2: Regulatory Framework & User Stories

1. Morning (9:00–12:30) – HIPAA Essentials & Checklist

- Read "HIPAA Privacy Rule Overview" on HHS.gov (30 min): https://bit.ly/HHS-HIPAA-PR
- Watch "HIPAA Compliance Basics" by GreyCampus (15 min): https://bit.ly/GC-HIPAA
- Build a **HIPAA Compliance Checklist** in Google Sheets:
  - Rows: "Requirement," "Implementation Approach," "Status."
  - Include: PHI de-identification, encryption, audit trails, BAA.
- **Artifact:** Sheet "HIPAA Checklist."

2. Afternoon (13:30–17:00) – User Story Workshop

- Learn user stories format (15 min): https://bit.ly/Agile-UserStories
- Draft **6 user stories** in Trello:
  - Example: "As a clinician, I want a one-para summary so that I can review patient history faster."
- Prioritize via **MoSCoW** (Must/Should/Could/Won't).
- Review with a mentor (30 min Zoom).

- **Artifact:** Trello board “User Stories & Prioritization.”

Day 3: Data Pipeline & De-Identification

1. Morning (9:00–12:30) – Data Source & De-ID Learning

- Register and explore MIMIC-III on PhysioNet (45 min): https://mimic.physionet.org/
- Read “De-identification of Clinical Text” by MITRE (20 min): https://bit.ly/MITRE-deid
- Clone MITRE deid repo: `git clone https://github.com/mitre/deid.git`
- Configure JSON rules for names/dates.

2. Afternoon (13:30–17:00) – Build De-ID Module

- Follow MITRE deid Quickstart (30 min).
- Run sample on 50 notes; verify no PHI (20 min).
- Document commands in a README.md.
- **Artifact:** GitHub repo “deid-module” with code and README.

Day 4: Embedding, Retrieval & RAG Integration

1. Morning (9:00–12:30) – Vector Store Setup

- Learn FAISS basics (20 min): https://bit.ly/FAISS-Guide
- Install `faiss-cpu` and `sentence-transformers`:

  ```
  pip install faiss-cpu sentence-transformers
  ```

- Choose model: `sentence-transformers/all-mpnet-base-v2`.

2. Afternoon (13:30–17:00) – RAG Pipeline

- Follow Hugging Face RAG quickstart (30 min): https://bit.ly/HF-RAG-Quick
- Write Python script to:
  1. Embed de-identified notes into FAISS.
  2. Query vector store.
  3. Feed retrieved docs into `google/flan-t5-small` for summary.
- Test with 5 clinical note examples.
- **Artifact:** Jupyter Notebook `rag_pipeline.ipynb`.

Day 5: Security, Encryption & Audit Trails

1. Morning (9:00–12:30) – Encryption Learning & Vault Setup

- Read HashiCorp Vault OSS intro (20 min): https://bit.ly/Vault-Intro
- Install Vault Dev: `brew install vault` or Windows MSI.
- Start dev server: `vault server -dev`.
- Learn basic KMS operations (15 min).

2. Afternoon (13:30–17:00) – Encrypt Vector Store & Logging

- Modify pipeline to encrypt FAISS index with Vault-issued key.
- Learn simple audit logging in Python (15 min): https://bit.ly/Py-Logging
- Implement logs: write JSON entries on each `/summarize` call (user_id, timestamp, note_id).
- Store logs in append-only file.
- **Artifact:** Updated `rag_pipeline.ipynb` with encryption and logging sections.

Day 6: Frontend Prototype & API

1. Morning (9:00–12:30) – Wireframes & React Scaffold

- Learn Figma basics (15 min): https://bit.ly/Figma-GettingStarted
- Wireframe Login, Upload, Summary view.
- Scaffold React app:

  ```
  npx create-react-app rag-ui
  cd rag-ui
  npm install tailwindcss
  ```

2. Afternoon (13:30–17:00) – Flask API & JWT Auth

- Learn Flask quickstart (20 min): https://bit.ly/Flask-Quickstart
- Install dependencies: `pip install flask pyjwt flask-cors`.
- Implement:
  - `/login` (hard-coded demo user + JWT).
  - `/summarize` (verifies JWT, calls pipeline notebook).
- Test with Postman (export collection).
- **Artifact:** GitHub repos `rag-ui` and `rag-api`.

Day 7: Integration, Testing & Demo

1. Morning (9:00–12:30) – Dockerize & Local Deploy

- Learn Docker basics (20 min): https://bit.ly/Docker-GetStarted
- Write `Dockerfile` for API and UI; create `docker-compose.yml`.
- Launch: `docker-compose up --build`.

2. Afternoon (13:30–17:00) – Testing & Demo Prep

- Functional tests:
  - React: basic render test (Jest).
  - Flask: pytest for `/summarize` flow.
- Prepare **Demo Slides** (Vision → Architecture → Live Demo → Next Steps).
- Record a 5-min screen walkthrough (Loom free).
- **Artifact:**
  - Demo video link.
  - Slides PDF.

Outcome:
By Day 7's end, you will have:

- A working RAG summarization prototype (UI + API + secure pipeline).
- Core PM artifacts (Vision doc, compliance checklist, user stories, wireframes, backlog).
- Demo materials demonstrating your end-to-end product management mastery in digital health tech.

Key Drivers Behind the Rise of AI Clinical Documentation

The emergence of AI-powered clinical documentation tools stems from **soaring administrative burdens**, **clinician burnout**, and the need for **better patient–clinician interaction**.

1. Electronic Health Record (EHR) Overload
Clinicians now spend over half of their workday interacting with EHRs, leaving less time for direct patient care. Researchers found that administrative tasks occupy up to **55% of clinicians' work hours**. [2]

2. Time Spent Per Patient Encounter
On average, outpatient physicians dedicate **16 minutes and 14 seconds** per patient just to documentation, with **11%** of that time logged **after hours**. [3]

3. Growing Documentation Complexity
Regulatory demands and the shift from paper to digital have increased documentation

requirements. Nurses, for instance, now devote **19–35%** of their shifts to EHR entries—up from **9%** in paper-based systems.[3]

4. Economic Impact on Healthcare Systems
A 2022 study in NHS England reported clinicians spend **13.5 hours per week** on documentation—an increase of 25% over seven years—translating to an average cost of **£25,639 per person annually** in time value.[4]

5. Clinician Burnout and Well-Being
Excessive documentation contributes directly to burnout. In a 2020 survey, **85%** of UK healthcare professionals agreed that documentation burden fueled clinician exhaustion.[4]

Key Challenges for Clinicians, Patients and Healthcare Organizations

Clinician Challenges

- **After-Hours Work**: **77.42%** of healthcare professionals report finishing work later than desired or working from home to complete documentation.[5]
- **Professional Dissatisfaction**: Burdened clinicians are more prone to errors and report lower job satisfaction, undermining retention and care quality.[3]
- **Workflow Interruptions**: One in four EHR look-ups fails to yield clear data, forcing clinicians to spend up to **62 minutes daily** searching for information.[4]

Patient-Facing Issues

- **Reduced Face-to-Face Time**: As documentation time rises, patient engagement diminishes, hurting satisfaction and trust.[2]
- **Continuity of Care Risks**: Incomplete or delayed notes can lead to miscommunication, fragmented care, and medical errors.[6]
- **Delayed Decision-Making**: Slow record availability hampers timely interventions, especially in acute or emergency settings.[3]

Organizational Concerns

- **Revenue Loss**: Poor documentation contributes to under-coding and claim denials; AI-driven Clinical Documentation Improvement (CDI) programs have shown to recover thousands in missed revenue per physician annually.[7]
- **Compliance & Legal Risk**: Inadequate records increase exposure to audits, penalties, and liability claims. Tightening regulations demand more rigorous documentation standards.
- **Operational Efficiency**: Excessive time on documentation translates into staffing inefficiencies and higher labor costs—over **£10,000 per person per year** just on information retrieval.[4]

Sources:
55% of clinicians' workdays on EHRs[2]
16m14s per encounter; 11% after hours[3]
19–35% shift documenting vs. 9% on paper[3]
13.5 h/week on documentation; £25,639/year[4]
85% cite burden → burnout[4]
77.42% finish work late due to documentation[5]

⁂

Key US Healthcare Facts Driving AI Clinical Documentation

Core Problem Statistics from US Credible Sources

1. Time Burden on US Physicians

- **Average daily EHR time**: US physicians spend **4.5 hours daily** on electronic health records[22]
- **Per encounter documentation**: Physicians spend an average of **16 minutes and 14 seconds per patient encounter** using EHRs[23]
- **Weekly EHR commitment**: Physicians spend **5.8 hours on EHR work for every 8 hours** of scheduled patient care[24]
- **After-hours work**: Primary care physicians spend **2.7 hours of personal time** daily on EHR tasks outside scheduled patient hours[24]

2. US Physician Burnout Crisis

- **Current burnout rates**: **45.2%** of US physicians reported at least one symptom of burnout in 2023, down from a peak of **62.8%** in 2021[25]
- **Peak pandemic impact**: Burnout reached an all-time high of **62.8%** during the height of COVID-19 in 2021[26]
- **Economic cost**: Physician burnout costs the US healthcare system **$4.6 billion annually** due to turnover and reduced work hours[27]
- **Specialty variations**: Emergency medicine leads with **56.5%** burnout, followed by internal medicine (**51.4%**), OB/GYN (**51.2%**), and family medicine (**51%**)[28]

3. Documentation Burden Impact

- **Patient care time**: Only **66.5%** of physician time is spent on direct patient care, while **20.7%** goes to EHR input[29]
- **Documentation perception**: **74.8%** of healthcare professionals believe documentation burden impedes patient care[30]
- **Work-life balance**: **77.42%** of healthcare professionals report finishing work later than desired due to documentation requirements[30]

- **International comparison**: US physicians spend **4 times longer** on EHR documentation compared to other countries[31]

4. Administrative Cost Crisis

- **Hospital administrative burden**: Administrative costs now account for **more than 40%** of total hospital expenses[32]
- **Healthcare waste**: Approximately **25%** of healthcare spending in the US is considered wasteful[33]
- **Claims denials**: Care denials increased **20.2%** for commercial and **55.7%** for Medicare Advantage claims between 2022-2023[32]
- **Overturned denials**: **75%** of care denials are eventually overturned, indicating inappropriate initial rejections[32]

Key Drivers Behind AI Clinical Documentation Emergence

1. EHR System Overload

- **Adoption rate**: **90%** of office-based physicians now use EHR systems[22]
- **Documentation complexity**: US outpatient notes are approximately **4 times longer** than those in other countries[31]
- **Multiple system burden**: Physicians must navigate complex regulatory requirements while maintaining quality care

2. Workforce Shortage Crisis

- **Projected deficit**: The US will face a shortage of **86,000 physicians by 2036** according to AAMC projections[34]
- **Retention challenges**: High burnout rates directly correlate with physician turnover and reduced clinical hours[34]

3. Quality of Care Concerns

- **Patient interaction reduction**: Excessive documentation time reduces face-to-face patient engagement[31]
- **Medical error risk**: Physician burnout increases the risk of medical errors and decreases patient satisfaction[34]
- **Care delays**: Poor documentation processes can lead to treatment delays and fragmented care[31]

Sources:
American Medical Association (AMA), Journal of the American Medical Association (JAMA), Mayo Clinic Proceedings, American Medical Informatics Association (AMIA), National Center for Biotechnology Information (NCBI), and Department of Health and Human Services (HHS) studies and reports.

⁂

Users of AI-Powered Clinical Documentation

Clinicians
Physicians, nurse practitioners, physician assistants, and other providers leverage AI documentation tools to streamline note-taking, reduce administrative workload, and focus more on patient interaction.

Medical Scribes & Documentation Specialists
Dedicated scribes or documentation teams use AI to automate transcription and summarization, enabling them to manage larger caseloads with greater accuracy and consistency.

Clinical Coders & Revenue Cycle Teams
Coding professionals rely on AI-generated structured summaries to ensure accurate ICD-10 and CPT code assignment, minimizing claim denials and optimizing reimbursement.

Nurses & Allied Health Professionals
Nurses, therapists, and technicians use AI to document vital signs, care plans, and procedural notes more efficiently, improving care coordination and record accuracy.

Compliance & Quality Assurance Officers
Regulatory and compliance staff use AI audit logs and summary reports to monitor documentation completeness, adherence to standards, and identify areas for training or process improvement.

Health IT & EHR Administrators
Technical teams integrate and manage AI modules within EHR platforms, oversee data pipelines, ensure system uptime, and enforce security and privacy controls.

Researchers & Data Analysts
Clinical researchers and informaticists utilize de-identified, AI-generated documentation datasets to study treatment outcomes, population health trends, and quality metrics without exposing PHI.

what are the success metrics for AI RAG based clinical documentation tool

AI RAG clinical documentation tools should be measured on retrieval quality, summary quality, clinical safety, workflow impact, and compliance/security, using a mix of automated metrics and human clinical review tailored to medical use cases.[59] [60] [61] [62]

Retrieval effectiveness

- Top-k retrieval precision/recall: Measure whether the system fetches clinically relevant passages that support each section of the note (e.g., HPI, Assessment/Plan) using precision@k/recall@k and coverage of guideline/evidence snippets in the retrieved context.[60] [59]

- Faithful grounding rate: Share of generated sentences whose facts can be traced to retrieved chunks (“attribution/groundedness” via RAGAS-style metrics or chunk attribution) to minimize hallucinations in medical settings.[63] [60]
- Retrieval latency: 95th-percentile time to retrieve supporting context per query, since slow retrieval degrades clinician usability in live encounters.[60]

Generation quality (summary)

- Clinical correctness and completeness: Human clinician ratings comparing summaries to source notes for absence of errors (precision) and inclusion of all clinically significant details (recall), as used in reader studies showing LLMs can match or exceed human baselines on completeness/correctness in clinical summarization.[64] [61]
- Hallucination rate: Proportion of unsupported or clinically unsafe statements in the generated note, assessed via expert review and automated groundedness checks common in medical RAG evaluations.[64] [60]
- Conciseness/readability: Clinician Likert ratings for brevity and clarity alongside length-normalized scores (e.g., sentences per problem) used in clinical reader studies of dialogue and note summarization.[61] [64]
- Task-specific NLP metrics: Use domain-aware metrics cautiously (e.g., ROUGE/BERTScore) supplemented with clinical relevance checks; literature recommends combining automated metrics with expert evaluation for clinical notes.[65] [62] [61]

Clinical workflow impact

- Documentation time reduction: Change in average minutes to complete notes per visit or per day after deployment of ambient/RAG tools, a primary endpoint in ambient scribe evaluations showing improved efficiency and reduced mental burden.[66]
- After-hours EHR time delta: Reduction in “pajama time” spent finalizing notes outside scheduled hours, a key burden outcome tracked in AI scribe studies and EHR-use evaluations.[67] [66]
- Edit burden: Percentage of AI-generated note tokens edited by clinicians and number of revision cycles before sign-off, recommended in emerging ambient scribe evaluation frameworks.[68] [65]
- Adoption and satisfaction: Clinician Net Promoter Score, System Usability Scale, and specialty-specific acceptance metrics proposed for standardized evaluation of ambient documentation tools.[65] [68]

Clinical safety and quality

- Safety-critical error rate: Frequency of errors with potential for clinical harm (e.g., wrong medication, dose, allergy, diagnosis), flagged via expert review protocols emphasized in clinical LLM/RAG assessments.[62] [64]
- Guideline and citation conformity: Rate at which generated assessments/plans align with retrieved guidelines or literature (traceable with citations), a priority in medical RAG reviews

to ensure evidence-based outputs.[59] [60]

- PHI leakage check: Automated scans confirming no identifiable patient data appears in training/evaluation artifacts, aligned with best practices for clinical text summarization research.[61] [62]

Retrieval–generation coherence (RAG-specific)

- Context utilization score: Degree to which the model uses retrieved passages in the final note (overlap/attention or semantic similarity between generated statements and retrieved chunks), highlighted in medical RAG evaluations.[59] [60]
- Negative retrieval robustness: Performance when distractor or conflicting passages are present, testing RAG's ability to prioritize authoritative clinical sources as recommended in RAG evaluations.[60] [59]
- Freshness/recency adherence: Share of outputs grounded in up-to-date sources when current guidance is retrieved, a noted requirement for safe medical RAG.[59] [60]

Operational performance

- End-to-end latency: Time from transcript/inputs to finalized draft note at the 95th percentile, a practical constraint in clinic workflows emphasized by medical RAG implementers.[60]
- Uptime and failure rates: Session-level success percentage and API error rates during clinical sessions, included in proposed ambient scribe evaluation frameworks.[68]
- Cost per note: Compute and infrastructure cost per finalized note as part of real-world feasibility evaluations for medical RAG systems.[59] [60]

Validation methodology

- Dual-track evaluation: Combine automated metrics (retrieval and generation) with blinded clinician reader studies across specialties to reflect real clinical priorities, as recommended by systematic studies and frameworks for clinical summarization and ambient scribing.[62] [61] [68]
- Benchmarking datasets: Use public, clinically annotated corpora (e.g., MACCROBAT for medical reports) and domain tasks when evaluating medical RAG pipelines, as demonstrated in medical RAG tutorials and endpoints.[60]
- Standardization need: Literature calls for standardized, specialty-aware metric suites that integrate accuracy, safety, usability, and workflow outcomes for AI documentation tools.[69] [65] [68]

⁂

provide in crisp with measure values as well

Here are crisp, clinically relevant success metrics for a RAG-based AI clinical documentation tool, with target values grounded in recent studies and accepted RAG evaluation practice.

Retrieval and grounding

- Context precision/recall: ≥0.80 precision@5 and ≥0.80 recall@20 on canonical note sections to ensure relevant evidence is retrieved for each generated statement.[80] [81]
- Groundedness/faithfulness score: ≥0.85 groundedness (RAGAS/deepset-style) with ≤5% unsupported claims per note to minimize hallucinations in clinical text.[82] [81]
- Retrieval latency: ≤300 ms p95 per query to avoid slowing real-time drafting during visits.[81]

Generation quality and safety

- Time in notes reduction: 10–20% decrease in "time in notes per appointment" within 3 months post-implementation; example: 6.2 → 5.3 minutes (−14.5%, P<.001) in a 100-clinician study of ambient AI.[83] [84]
- Edit burden: ≤20% of AI-generated tokens edited prior to sign-off; observational work shows typed share dropped ~30% with ambient AI (11.2% → 7.9%) indicating higher automation of draft content.[85]
- Safety-critical error rate: 0 serious errors per 100 notes on adjudicated review; minor factual error rate ≤2 per 100 notes with mandatory grounding to retrieved context.[86] [87]
- Readability/conciseness: Clinician Likert ratings ≥4/5 for clarity and organization in reader studies of clinical summarization.[87] [88]

Clinician well-being and workflow

- Burnout reduction: 10–20 percentage point absolute reduction in burnout prevalence at 8–12 weeks among active users; example: −21.2 points at Mass General Brigham (MGB) in 84 days with ambient documentation tech.[89] [90]
- After-hours EHR time ("pajama time"): 10–20% reduction vs. baseline; some systems report 3 fewer hours/week among regular AI scribe users, though effects can vary across sites.[91] [92]
- Adoption and satisfaction: Net Promoter Score ≥30 and System Usability Scale ≥80 indicating strong clinician acceptance in ambient scribe frameworks.[93] [94]

Operational and cost

- End-to-end latency: Draft note available ≤60 seconds p95 from encounter end to support same-day completion.[81]
- Uptime and reliability: ≥99.5% service uptime; API error rate ≤1% per 1000 sessions in clinic settings per proposed evaluation frameworks.[93]
- Cost per finalized note: Target ≤$1–$2 at pilot scale (compute + storage), to remain economically viable in ambulatory use; track as a KPI alongside time savings.[95] [81]

Validation approach

- Dual-track evaluation: Blend automated metrics (precision/recall, groundedness) with blinded clinician reader studies across specialties for safety and completeness, as recommended by recent clinical summarization and ambient-scribe research.[88] [87] [93]
- Report deltas with confidence: Present pre/post changes (e.g., time in notes, after-hours) with 95% CIs and P-values to meet clinical evidence standards used in JAMA Network Open studies of ambient documentation.[84] [83]

⁂

basis the existing AI clinical documentation systems based on RAG, tell what is benchmark success metrics

Benchmark success metrics for RAG-based AI clinical documentation, drawn from US health-system deployments and peer-reviewed studies:

Time and workflow

- Time in notes per appointment: 6.2 → 5.3 minutes (−14.5%, P<.001) at 3 months post-implementation in a 100-clinician JAMA Network Open study of an ambient AI documentation platform.[106] [107]
- After-hours EHR time: No significant change in one JAMA Network Open study (38.2 → 39.8 minutes, P=.14), indicating site- and workflow-dependent impact that should be tracked separately from “time in notes”.[107] [106]
- Scale and adoption: Enterprise rollout from 850-person pilot to 2,700+ active users at Mass General Brigham, highlighting feasibility and viral adoption in large US systems.[108]

Clinician well-being

- Burnout reduction: 21.2 percentage-point absolute reduction in burnout prevalence at 84 days among active users in Mass General Brigham program reports and coverage (enterprise survey).[109] [110] [111]
- Cognitive load and satisfaction: Significant reductions in mental demand/effort and improved work satisfaction documented alongside time savings in JAMA Network Open evaluation of ambient AI.[106] [107]

Document quality and editing

- Note length vs. effort: Despite reduced time, mean note characters increased (~4,326 → ~4,548; P=.01) and progress note length increased (~5,683 → ~5,961; P<.001), implying higher completeness without extra time burden.[106]
- Edit burden (practical benchmark): Track share of AI-generated text modified before sign-off; emerging frameworks recommend targeting ≤20% edited tokens to indicate high-quality drafts, though specific percentages vary by site and specialty.[112]

RAG retrieval and grounding (model quality)

- Groundedness/faithfulness: Target ≥0.85 groundedness with ≤5% unsupported claims per note using RAG evaluation toolchains (e.g., RAGAS/groundedness scoring) in medical RAG assessments and tutorials.[113] [114]
- Retrieval precision/recall: Operational benchmark ≥0.80 precision@5 and ≥0.80 recall@20 on section-level evidence retrieval to ensure clinically relevant context feeding generation, per medical RAG evaluation practices.[114] [113]
- Robustness scenarios: Evaluate negative rejection, noise robustness, and integration per emerging medical RAG benchmarks (e.g., MedRGB/MIRAGE) as part of acceptance criteria before clinical pilots.[115] [116]

Operational performance

- End-to-end latency: Draft note availability within ≤60 seconds at p95 from encounter end for clinic usability; retrieval p95 ≤300 ms to avoid interactive lag during drafting.[114]
- Reliability: ≥99.5% service uptime and ≤1% session-level API error rate recommended in ambient scribe evaluation frameworks for safe clinical operations at scale.[112]

Program outcomes (real-world evidence exemplars)

- System-level hours saved: Large groups report thousands of clinician hours saved (e.g., AMA coverage of 15,000 hours saved over 2.5 million uses) as a program KPI; track locally as “hours returned to care”.[117]
- Career sustainability signal: 60% of clinicians in an MGB pilot reported being likely to extend career length due to ambient documentation technology, an adoption and well-being composite indicator for leadership reporting.[108]

Methodology notes for benchmarking

- Use pre/post EHR telemetry and blinded reader studies: Pair time-in-notes and after-hours metrics with clinician ratings of accuracy, clarity, and safety to meet evidence standards shown in JAMA Network Open ambient AI studies.[118] [106]
- Report with statistics: Present deltas with 95% CIs and P-values; stratify by specialty and clinician demographics given heterogeneous effects observed in US deployments.[118] [106]

⁂

how much should be hit rate

Short answer: For a clinical RAG documentation tool, a practical “hit rate” (at least one clinically relevant chunk retrieved in top-k) benchmark is ≥0.9 @k=5, with section-level precision@5 ≥0.8 and recall@20 ≥0.8; top-1 inclusion of the gold supporting snippet can target ≥0.75 based on medical RAG benchmarks and reviews.[128] [129] [130] [131] [132]

Details and targets

- Hit rate@5 (at least one relevant passage in top 5): ≥0.90 for core sections like HPI, Assessment, and Plan in internal validation sets to ensure reliable grounding during note generation.[128]

- Precision@5: ≥0.80 to keep retrieved context mostly relevant and reduce hallucination risk in downstream generation, consistent with medical RAG evaluation guidance and practitioner playbooks.[133] [132]
- Recall@20: ≥0.80 to capture most clinically necessary details when broader context is needed for completeness in summaries, per medical RAG evaluation practice.[132] [133]
- Top-1 gold-support inclusion: 0.75–0.80 feasible; medical RAG studies report ~79.6% of ground-truth snippets identified at rank 1 on PubMedQA-like tasks, informing a strong operational target for clinical retrieval.[130] [131]
- Ranking quality (MRR/nDCG): MRR ≥0.80 and nDCG@10 ≥0.85 when graded by clinician relevance scales, to ensure the most useful evidence appears early and is actually used in generation.[134] [135]
- Groundedness linkage: With the above retrieval targets, end-to-end groundedness (share of generated claims supported by retrieved context) should hit ≥0.85 with ≤5% unsupported statements per note in clinical RAG evaluations.[129] [132]

Why these numbers: Medical RAG benchmarks (e.g., MIRAGE/MedRAG) show high top-1 identification of gold snippets and improving accuracy with modest k before noise hurts performance, supporting ≥0.75 top-1 and high hit rate@5 goals for safe clinical use; operational guides emphasize precision/recall trade-offs to maintain safety and latency in production.[131] [133] [130] [132]

⁂

help create a risk register for RAG based AI clinical documentation tool product development using NIST RMF

Yes. Below is a ready-to-use NIST RMF–aligned risk register template for a RAG-based AI clinical documentation product, including how to fill it, example entries mapped to NIST SP 800-53 Rev.5 controls, and where this fits in each RMF step.

Overview: how RMF drives the risk register

- NIST SP 800-37 Rev.2 defines a 7-step lifecycle: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor, and the risk register is created in Prepare/Categorize and maintained through Monitor.[143] [144] [145]
- Security controls come from NIST SP 800-53 Rev.5's catalog (e.g., Access Control AC, Audit AU, Identification and Authentication IA, System and Information Integrity SI, Privacy controls), which the register maps to each risk and treatment.[146] [147] [148]
- For HIPAA-aligned systems processing ePHI, use NIST SP 800-66 Rev.2 guidance to inform safeguards and risk handling alongside RMF artifacts.[149]

Risk register structure (fields and instructions)

- Fields to include: Risk ID, RMF Step, System Category (FIPS 199), Description, Cause/Threat, Vulnerability, Impact (H/M/L), Likelihood (H/M/L), Inherent Risk Rating, Affected Assets/Data, Applicable 800-53 Controls, Existing Controls, Control Gaps, Mitigation/Response Plan, Risk Owner, Target Residual Risk, Due Date, Status, Monitoring Metric/Trigger, POA&M ID.[144] [145] [143]
- Categorize the AI system using FIPS 199 (e.g., Confidentiality=Moderate/High; Integrity=High; Availability=Moderate for clinical documentation), then select 800-53 baselines and tailor controls to address identified risks, recording choices in the register and System Security Plan (SSP).[145] [147] [143]

Example risks tailored to a clinical RAG documentation tool

1. PHI exposure via retrieved context or generated note

- Description: RAG retrieves clinical text; misconfiguration or prompt injection could surface PHI to unauthorized users or logs; generation could leak identifiers if de-identification fails.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: AC-2, AC-3, AC-6 (access control), IA-2 (MFA), SC-13/SC-28 (encryption at transit/at rest), SI-10 (information input validation), AU-2/AU-12 (audit logging), AR family privacy controls; HIPAA implementation via 800-66 r2.[147] [148] [149]
- Mitigation: Enforce RBAC/ABAC, JWT+MFA, encrypt FAISS indexes and transcripts, PHI redaction before indexing, prevent context logging, implement data minimization and privacy screens, audit retrievals and generations; document in SSP and POA&M.[143] [149] [147]
- Monitoring: Weekly audit of access logs, DLP scans on outputs, automated tests for PHI leakage; trigger thresholds in SIEM.
- RMF linkage: Select/Implement/Assess/Monitor.

2. Model hallucination producing unsafe or incorrect clinical statements

- Description: Generated summaries include unsupported or incorrect recommendations impacting clinical safety.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: SA-8/SA-11 (developer security testing/verification), RA-5 (vulnerability scanning adapted for model eval), SI-4 (monitoring), PL-2 (security plan with eval criteria), SR-11 (supply chain—model provenance), IR-4 (incident handling for harmful outputs).[148] [147]
- Mitigation: Retrieval constraints, groundedness checks, clinician-in-the-loop sign-off, blocklists for medication/dose changes without citations, evaluation gates with acceptance criteria; record testing in SAR and conditions in ATO package.[147] [143]
- Monitoring: Track groundedness ≥0.85 and ≤5% unsupported claims per note; alert on safety-critical entities; continuous model evaluation calendar.
- RMF linkage: Select/Implement/Assess/Authorize/Monitor.

3. Prompt injection or adversarial context poisoning

- Description: Malicious text in notes or imported documents manipulates RAG prompts to exfiltrate data or suppress guardrails.

- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: SI-10 (input validation), SI-4 (monitoring), SC-7 (boundary protection), SC-18 (mobile code restrictions), SR family (supply chain).[148] [147]
- Mitigation: Content sanitization, allowlist-only instruction patterns, chunk-level trust scores, retrieval source whitelisting, disable tool-use side effects, adversarial testing in Assess step.
- Monitoring: Injection detection heuristics and anomaly alerts; monthly red-team tests.
- RMF linkage: Select/Implement/Assess/Monitor.

4. Unauthorized access and weak identity governance

- Description: Inadequate IAM enables unauthorized use of transcripts, indexes, or audit logs.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: AC-2/AC-3/AC-6 (account/least privilege), IA-2 (MFA), IA-5 (authenticator management), AU-6 (audit review), CM-5 (access restrictions).[147] [148]
- Mitigation: Centralized IAM, MFA, least privilege for microservices, quarterly access recertification, segregation of duties, audit trail reviews.
- Monitoring: Weekly IAM anomalies; quarterly recertification attestations.
- RMF linkage: Select/Implement/Assess/Monitor.

5. Inadequate auditability and chain-of-custody for clinical outputs

- Description: Missing or mutable logs obstruct incident investigation and compliance attestations.
- Impact/Likelihood: Impact Medium/High, Likelihood Medium; Inherent Risk High.
- Controls: AU-2/AU-3/AU-6/AU-8/AU-9/AU-12 (audit generation, protection, time sync, retention), PE/MP when applicable.[148] [147]
- Mitigation: Immutable, time-synced logs, append-only storage, tamper-evident hashing; retention policies in SSP; periodic SAR checks.
- Monitoring: Log integrity verification jobs; SIEM correlation rules.
- RMF linkage: Select/Implement/Assess/Monitor.

6. Data retention, minimization, and HIPAA alignment gaps

- Description: Over-retention of transcripts or indexes increases breach impact; unclear privacy notices or consent flows.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: PL-2 (plans), MP family (media), DM/AR privacy controls per 800-53 Rev.5 and HIPAA implementation per 800-66 r2.[149] [147]
- Mitigation: Data retention schedule, de-identification before model training, consent management UI, BAAs with third parties; document in Privacy Plan.
- Monitoring: Monthly retention purges and audits; privacy incident drills.
- RMF linkage: Prepare/Categorize/Select/Implement/Monitor.

7. Third-party and supply chain (models, vector DB, speech services)

- Description: Vulnerabilities or noncompliance in external components handling ePHI.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: SR-3/SR-4 (provenance, tamper resistance), SA-9 (external services), CA-3 (system interconnections), RA-3 (risk assessment of suppliers).[150] [147]
- Mitigation: BAAs where applicable, SBOMs, version pinning, vulnerability scanning, vendor risk assessments; interconnection agreements documented.
- Monitoring: Quarterly supplier assessments; auto alerts for CVEs.
- RMF linkage: Select/Implement/Assess/Monitor.

8. Model/data drift degrading clinical accuracy

- Description: Performance declines as clinical patterns change, risking unsafe summaries.
- Impact/Likelihood: Impact Medium/High, Likelihood Medium; Inherent Risk Medium/High.
- Controls: CM-3 (configuration change control), SI-12 (ML-specific monitoring can be documented under SI/RA), PL-2 (plans for evaluation cadence).[147]
- Mitigation: Scheduled re-evaluation with clinical test sets, drift dashboards, rollback plan, A/B holdouts.
- Monitoring: Alert on KPI thresholds (groundedness, edit burden, error types).
- RMF linkage: Assess/Monitor.

9. Incident response gaps for AI-specific failures

- Description: Lacking runbooks for PHI leakage, harmful outputs, or compromised embeddings.
- Impact/Likelihood: Impact High, Likelihood Medium; Inherent Risk High.
- Controls: IR-4/IR-5/IR-6 (response, monitoring, reporting), CP-2 (contingency plan).[148] [147]
- Mitigation: AI-specific IR playbooks, breach notification workflows, tabletop exercises; map to HIPAA breach requirements in SSP/Privacy Plan.
- Monitoring: Quarterly tabletop results and POA&M updates.
- RMF linkage: Implement/Assess/Authorize/Monitor.

10. Availability and latency SLO breaches impacting care

- Description: Excessive latency or downtime disrupts clinics and pushes work after hours.
- Impact/Likelihood: Impact Medium/High, Likelihood Medium; Inherent Risk Medium/High.
- Controls: CP-10 (recovery), SC-5 (QoS), SI-4 (monitoring), AU for performance events, SA-11 for performance testing.[147] [148]
- Mitigation: Capacity planning, circuit breakers, fallbacks to manual templates, DR plans, SLOs in runbooks; test in Assess phase.
- Monitoring: SLO dashboards; on-call paging for p95>target.
- RMF linkage: Implement/Assess/Monitor.

How to use this in each RMF step

- Prepare: Establish roles (Risk Executive, AO, ISSO), define risk tolerance, select tooling (risk register in GRC or spreadsheet), and draft evaluation strategy for AI systems, capturing initial risks above.[144] [145] [143]
- Categorize: Apply FIPS 199 impact levels for confidentiality, integrity, availability given ePHI processing, and document in the register and SSP context.[145] [143]
- Select: Choose 800-53 baselines (e.g., Moderate/High) and tailor with privacy controls; map each selected control to specific risks in the register with planned mitigations.[148] [147]
- Implement: Configure controls (IAM, encryption, logging, IR playbooks), reference control IDs per risk, and note evidence locations (configs, policies) in the register.[147] [148]
- Assess: Conduct control assessments and model evaluations; record findings, severity, and POA&M items tied to specific risk IDs in the register.[143] [145]
- Authorize: Compile SSP, SAR, POA&M; present residual risk and acceptance rationale linked to the register to obtain ATO from the Authorizing Official.[145] [143]
- Monitor: Continuously track metrics (e.g., groundedness ≥0.85, PHI leakage=0, uptime ≥99.5%), update risk statuses, and maintain POA&M closures per cadence.[143] [147]

Starter risk register template (copy-ready headers)

- Columns: Risk ID | RMF Step | FIPS 199 (C/I/A) | Risk Description | Threat | Vulnerability | Impact (H/M/L) | Likelihood (H/M/L) | Inherent Risk | Affected Assets/Data | Applicable 800-53 Controls | Existing Controls | Control Gaps | Mitigation Plan | Evidence/Artifacts | Risk Owner | Target Residual Risk | Due Date | Status | Monitoring Metric/Trigger | POA&M ID [143] [147] [145].

Control families most relevant to RAG clinical documentation

- Access Control (AC), Identification and Authentication (IA), Audit and Accountability (AU), System and Communications Protection (SC), System and Information Integrity (SI), Planning (PL), Risk Assessment (RA), Incident Response (IR), Configuration Management (CM), Contingency Planning (CP), and Supply Chain (SR), with privacy and HIPAA guidance via SP 800-66 r2.[149] [148] [147]

Where to document and store

- System Security Plan (SSP) and Privacy Plan reference the risk register and controls; the Security Assessment Report (SAR) and POA&M reference the same risk IDs and remediation steps, ensuring RMF traceability end-to-end.[145] [143]

References

- NIST SP 800-37 Rev.2 (RMF core process).[143]
- Practitioner guides summarizing the seven RMF steps and artifacts.[144] [145]
- NIST SP 800-53 Rev.5 (security and privacy controls catalog).[146] [148] [147]
- NIST SP 800-66 Rev.2 (HIPAA Security Rule implementation guidance).[149]

⁂

explain in easiest languugage completely this - NIST SP 800-66 Rev.2

NIST SP 800-66 Rev.2, in plain English: it's the official, practical "how-to" guide from NIST for meeting HIPAA's Security Rule when handling electronic protected health information (ePHI) in the U.S. It explains what the HIPAA Security Rule expects, then shows exactly how to assess risks, choose safeguards, implement them, and keep them working over time, tailored to an organization's size and complexity.[163] [164]

What it covers at a glance

- Purpose: Help covered entities and business associates protect ePHI by translating HIPAA Security Rule requirements into actionable security and privacy practices, checklists, and references.[164] [163]
- Audience: Any HIPAA-regulated entity handling ePHI (providers, health plans, clearinghouses, and their vendors), from small clinics to large health systems and cloud/service providers under Business Associate Agreements.[163] [164]
- Nature: Guidance, not a law—HIPAA is the law; 800-66 shows practical ways to comply and points to aligned NIST frameworks and control catalogs to implement safeguards consistently.[164] [163]

Core ideas in the guide

- Risk-based approach: Do a risk assessment focused on threats and vulnerabilities to ePHI, set risk tolerance, then select reasonable and appropriate safeguards for confidentiality, integrity, and availability—scaled to the organization's context.[165] [163]
- Map HIPAA to controls: It cross-walks HIPAA Security Rule standards and implementation specs (administrative, physical, technical) to recognizable security controls and practices, helping teams move from requirements to concrete actions.[163] [164]
- Lifecycle mindset: Protecting ePHI isn't one-and-done—plan, implement, test, train, monitor, and improve continuously, aligning with NIST's broader risk frameworks and control catalogs.[166] [163]

How it relates to other NIST resources

- NIST RMF (SP 800-37): A step-by-step process for managing system risk; 800-66 shows how to apply that process for HIPAA Security Rule compliance in healthcare contexts.[166] [163]
- NIST SP 800-53 Rev.5: The detailed library of security and privacy controls (e.g., access control, encryption, audit logging); 800-66 points to selecting and tailoring these controls to satisfy HIPAA safeguards.[167] [168]
- NIST SP 800-30: Deep guidance for conducting the risk assessment that HIPAA requires; 800-66 leverages its methods to evaluate threats, likelihood, and impact to ePHI.[165] [163]

What's notably emphasized in Rev.2

- Practical resources and structure: Rev.2 adds clearer tables, appendices, and references (including online resources) to make implementation easier for organizations of all sizes, not just large IT teams.[164] [163]
- ePHI focus and accountability: It reinforces that regulated entities remain responsible for safeguarding ePHI even when using vendors; outsourcing processing doesn't outsource accountability under HIPAA.[163] [164]
- Alignment with modern frameworks: It aligns with the NIST Cybersecurity Framework and current control sets so healthcare entities can integrate HIPAA safeguards into enterprise cybersecurity programs rather than treating them as separate silos.[169] [163]

Plain-language breakdown of HIPAA safeguards as implemented via 800-66

- Administrative safeguards: Policies, risk assessments, workforce training, vendor oversight (BAAs), incident response, and contingency planning to manage security at the organizational level.[164] [163]
- Physical safeguards: Facility and device protections—secure locations, controlled access, workstation/device policies, and media handling to prevent physical loss or theft of ePHI.[163] [164]
- Technical safeguards: Access controls (unique IDs, MFA), encryption in transit/at rest, audit logs, automatic logoff, integrity controls, and transmission security to protect systems that store or transmit ePHI.[164] [163]

What to do step-by-step using 800-66 Rev.2

- Identify systems and data: List all places where ePHI is created, received, maintained, or transmitted (EHR, data lakes, backups, mobile, cloud), including third parties.[163] [164]
- Assess risk: For each system, evaluate threats (e.g., unauthorized access, ransomware, insider error), vulnerabilities (e.g., weak IAM, unencrypted storage), likelihood, and impact to ePHI; document results and priorities.[165] [163]
- Select safeguards: Choose reasonable and appropriate administrative, physical, and technical controls mapped from HIPAA requirements to NIST control families (e.g., AC, IA, SC, AU) and tailor to the environment.[167] [163]
- Implement and train: Configure controls (e.g., MFA, encryption, RBAC, audit), write policies, conduct workforce training, sign BAAs, and ensure vendors meet equivalent protections.[164] [163]
- Test and monitor: Review logs, run security tests, audit vendors, update risk assessments, and refine safeguards as systems and threats change—keep evidence for OCR audits.[163] [164]

Why teams use 800-66 Rev.2

- Translates HIPAA into action: It turns "what you must do" (HIPAA Security Rule) into "how you can do it" (controls and processes) in healthcare environments.[164] [163]
- Enables consistent audits: Aligning with NIST controls creates a common language for documenting safeguards, assessing effectiveness, and proving due diligence to regulators and partners.[167] [163]

- Scales to real-world constraints: The “reasonable and appropriate” standard lets small clinics and large systems adopt protections proportional to their risk and resources, while still meeting HIPAA.[163] [164]

If only one thing is remembered

- NIST SP 800-66 Rev.2 is the practical playbook for building, proving, and maintaining HIPAA Security Rule compliance for any system that touches ePHI—do a risk assessment, select and tailor controls, implement and train, then monitor and improve continuously, all with mappings to widely recognized NIST methods and controls.[166] [163]

⁂

Quiz me on this topic

Here’s a quick, progressive quiz on NIST SP 800-66 Rev.2 and HIPAA Security Rule implementation. Each question is concise and practical; answers can be checked in the cited sources.

Basics

1. What is the purpose of NIST SP 800-66 Rev.2, and who must follow HIPAA’s Security Rule? [177] [178]
2. What three properties of ePHI does the Security Rule protect, and how are they defined? [177]
3. Is NIST SP 800-66 legally binding, and does using it guarantee compliance? Explain.[177]

Structure and requirements
4) Name the three safeguard categories under the HIPAA Security Rule and give one example control from each.[177]
5) What is the difference between a required and an addressable implementation specification? How should addressable ones be handled?[177]
6) Where in 800-66 can sample questions/activities for standards like Access Control, Security Awareness, or Contingency Plan be found?[177]

Risk-based approach
7) What does 800-66 say about performing a risk assessment—does OCR prescribe a specific method? Which NIST doc guides the assessment?[179] [177]
8) How does 800-66 recommend mapping HIPAA Security Rule requirements into concrete safeguards or controls? Which NIST catalog is referenced?[178] [180]

Governance and lifecycle
9) Describe the “flexibility of approach” and how organization size/complexity affects safeguard selection. Cite the relevant HIPAA section.[177]
10) List four recurring lifecycle activities 800-66 expects beyond initial implementation (e.g., training, monitoring).[181] [178]

Technical safeguards specifics
11) Under 45 CFR 164.312, which implementation specs are listed for Access Control and

Transmission Security (identify which are Required vs Addressable)?[177]
12) What logging/audit expectations does 800-66 point to for demonstrating compliance over time?[177]

Vendors and BAAs
13) How does 800-66 address Business Associates—who remains accountable for ePHI when services are outsourced?[178] [181]
14) What documents should reflect vendor interconnections and responsibilities in a HIPAA program aligned to 800-66?[178]

Operationalization
15) Give three examples of evidence artifacts 800-66 expects organizations to maintain for OCR review.[181]
16) How should entities handle media sanitization and device/media controls—what NIST reference is commonly cited?[182]

Advanced/application
17) In a RAG-based AI clinical documentation tool, name two high-risk scenarios 800-66 would expect to be mitigated and the types of safeguards that align with HIPAA technical standards.[177]
18) How do 800-66 and SP 800-37 (RMF) complement each other when documenting risk, controls, and authorization decisions?[183] [178]

Answer key (high level)

1. Practical guidance to implement HIPAA Security Rule; all covered entities and business associates must comply with HIPAA; 800-66 helps them do so.[178] [177]
2. Confidentiality, integrity, availability as defined in 45 CFR 164.304; confidentiality = no unauthorized disclosure, integrity = not altered/destroyed, availability = accessible/usable on demand.[177]
3. Not a law; use does not guarantee compliance; it's guidance and a resource guide.[177]
4. Administrative, Physical, Technical; examples: risk management (admin), facility access controls (physical), access control/encryption (technical).[177]
5. Required must be implemented; addressable must be assessed and implemented if reasonable/appropriate or documented with alternative measures/rationale.[177]
6. Section 5 tables with key activities and sample questions (e.g., Tables 11–20).[177]
7. OCR does not prescribe a specific method; use NIST SP 800-30 for risk assessment methodology.[179] [177]
8. Map HIPAA standards to NIST SP 800-53 Rev.5 controls; select/tailor appropriate controls.[180] [178]
9. Flexibility of approach (164.306(b)) allows tailoring based on size/complexity/technical capabilities.[177]
10. Training, monitoring, evaluation, incident response, contingency planning, periodic risk re-assessment.[181] [178]

11. Access Control: Unique User Identification (R), Emergency Access Procedure (R), Automatic Logoff (A), Encryption/Decryption (A); Transmission Security: Integrity Controls (A), Encryption (A).[177]
12. Maintain audit controls and protected audit logs; time sync, retention, and review to demonstrate ongoing compliance.[177]
13. Covered entities remain accountable; BAAs required; outsourcing doesn't outsource responsibility.[181] [178]
14. System Security Plan, interconnection agreements, BAAs, policies/procedures.[178]
15. Risk assessment reports, policies/procedures, training records, audit logs, incident response documentation.[181]
16. NIST SP 800-88 for media sanitization under device/media controls.[182]
17. PHI leakage and unsafe generation; safeguards: access control, encryption, audit controls, integrity checks

⁂

summarize all action to be followed as mentioned in this framework - NIST SP 800-66 Rev.2

Here is a concise, action-oriented checklist of what to do under NIST SP 800-66 Rev.2 to implement the HIPAA Security Rule. Each line is a concrete action that a regulated entity (covered entity or business associate) should take, aligned to the guide's intent.

Program setup and scoping

- Identify all systems, apps, and vendors that create, receive, maintain, or transmit ePHI; draw data flows and interconnections, including cloud and mobile endpoints.[190] [191]
- Define roles and accountability (security officer, privacy officer, IT lead), and set risk tolerance aligned to leadership expectations and HIPAA obligations.[192] [190]
- Inventory all agreements with third parties; determine which are Business Associates and execute/update BAAs that bind them to HIPAA-equivalent safeguards.[193] [190]

Risk assessment and categorization

- Perform a HIPAA-focused risk assessment of threats, vulnerabilities, likelihood, and impact to ePHI; document methods, findings, and prioritization (NIST SP 800-30 methods are acceptable; OCR does not prescribe one "right" method).[191] [194]
- Categorize systems processing ePHI for confidentiality, integrity, availability and document rationale to drive "reasonable and appropriate" safeguards selection.[190] [191]

Control selection and mapping

- Map HIPAA Security Rule standards and implementation specifications to concrete safeguards using NIST's mappings to SP 800-53 Rev.5 controls and the NIST Cybersecurity Framework subcategories via CPRT/OLIR references.[195] [196] [190]

- For each implementation specification: if “required,” implement; if “addressable,” assess feasibility and either implement, implement an alternative, or document rationale for not implementing, with residual risk noted.[191]

Administrative safeguards (do-now actions)

- Establish policies and procedures covering access control, incident response, contingency planning, risk management, training, change management, and device/media handling; keep versioned evidence.[193] [191]
- Train workforce initially and periodically on Security Rule duties, phishing and ransomware risks, and ePHI handling; log attendance and content.[191]
- Manage third parties: due diligence, BAAs, onboarding risk reviews, and ongoing monitoring of business associates’ controls and breach notifications.[192] [190]

Physical safeguards (do-now actions)

- Control facility and workstation access; implement visitor procedures, device locks, and secure areas for servers and backups.[191]
- Protect and track devices/media that may store ePHI; apply secure storage and transport procedures; sanitize or destroy media at end of life per NIST 800-88 practices.[193]

Technical safeguards (do-now actions)

- Enforce unique user IDs, least privilege, MFA where appropriate, and automatic logoff; implement strong authentication and authorization for all ePHI systems.[191]
- Encrypt ePHI in transit and at rest; ensure keys are protected and encryption is validated against policy; document exceptions and compensating controls.[191]
- Enable audit logs for access, changes, and transmission of ePHI; protect logs from tampering; set retention and time synchronization; schedule regular reviews.[191]
- Implement integrity controls to detect improper alteration or destruction of ePHI; monitor for anomalous activity; patch and vulnerability-manage relevant systems.[191]

Operationalization and evidence

- Create and maintain the System Security Plan (SSP) and Privacy Plan that tie HIPAA requirements to selected controls, configurations, and responsible roles.[195] [190]
- Build incident response and breach notification runbooks aligned with HIPAA breach requirements; test via tabletop exercises and record lessons learned.[191]
- Develop contingency plans: backups, disaster recovery, and emergency mode operations; test restoration regularly and record results.[191]

Assessment and authorization

- Test and assess control effectiveness; collect artifacts (configs, screenshots, logs, policies, training records); record findings, severity, and remediation in a POA&M.[190] [191]
- Use NIST’s CPRT mappings and 800-53A-style assessment procedures to structure testing; resolve high-risk gaps before go-live or document risk acceptance by leadership.[196] [195]

Continuous monitoring and improvement

- Establish continuous monitoring: periodic risk reassessments, log reviews, vulnerability scanning/patching cadence, vendor reviews, and policy refresh cycles.[192] [190]
- Track KPIs/KRIs (e.g., failed logins, unencrypted endpoints, audit review completion, vendor assessment status); adjust safeguards as technology and threats evolve.[190] [192]
- Keep evidence current for OCR inquiries: risk assessment reports, BAAs, training logs, incident/breach records, audit logs, backup/restore tests, and policy attestations.[193] [191]

Where to find the official materials and mappings

- Official guide and supplemental materials page (with links to tables, tools, and mappings). [195] [190]
- Full PDF of SP 800-66 Rev.2 for detailed standards, implementation specs, and sample activities/questions (Section 5 tables).[191]
- NIST SP 800-53 Rev.5 for control catalog; use CPRT to see HIPAA-to-control mappings for faster tailoring.[196] [195]

Bottom line: Do a documented risk assessment, select and tailor safeguards mapped to HIPAA through NIST controls, implement and train, assess and authorize, then monitor and improve continuously—keeping thorough evidence for accountability and OCR readiness.[195] [190] [191]

⁂

can you do all of this for RAG based AI clinical documentation Tool, as a product manager to create a risk register

Yes. Below is a complete, copy-ready risk register for a RAG-based AI clinical documentation tool, structured as a product manager would maintain it under NIST RMF and mapped to HIPAA via NIST SP 800-66 Rev.2 and NIST SP 800-53 Rev.5. It includes fields, filled example risks, control mappings, mitigation plans, evidence, owners, and monitoring triggers.

Header fields to use
Risk ID | RMF Step | System (Boundary) | FIPS 199 (C/I/A) | Risk Description | Threat | Vulnerability | Impact (H/M/L) | Likelihood (H/M/L) | Inherent Risk (H/M/L) | Affected Assets/Data | Applicable HIPAA Safeguards | Applicable NIST 800-53 Controls | Existing Controls | Control Gaps | Mitigation/Response Plan | Evidence/Artifacts | Risk Owner | Target Residual Risk | Due Date | Status | Monitoring Metric/Trigger | POA&M ID [205] [206] [207].

Assumptions for categorization

- System processes ePHI; set FIPS 199 impacts: Confidentiality=High, Integrity=High, Availability=Moderate, documented in SSP and register context.[206] [205]

Risk entries

R-01 PHI exposure via retrieval/generation

- RMF Step: Select/Implement/Assess/Monitor.[205]

- Description: RAG retrieves clinical text; misconfiguration or logging could expose PHI; generated notes might include identifiers if de-identification fails.
- Threat: Unauthorized access, insider misuse, log leakage.
- Vulnerability: Insufficient RBAC/MFA, plaintext logs, PHI in embeddings.
- Impact: High | Likelihood: Medium | Inherent: High.
- Assets/Data: Vector DB (embeddings), transcripts, notes, logs.
- HIPAA Safeguards: Technical—Access Control, Audit Controls, Integrity, Transmission Security; Administrative—Risk Mgmt, Workforce Training.[206]
- NIST 800-53: AC-2/3/6, IA-2, SC-13/SC-28 (encryption), AU-2/6/9/12, SI-10, PL-2; privacy mappings via 800-66 Rev.2 Appendix tables/online CPRT.[208] [207] [209]
- Existing: Basic auth; HTTPS; app logs.
- Gaps: No MFA; logs may contain PHI; embeddings unencrypted.
- Mitigation: Enforce RBAC/least privilege; MFA; encrypt at rest (DB + embeddings) and in transit; PHI redaction before indexing; disable sensitive content in logs; DLP checks; BAA with any vendors handling ePHI; document in SSP.[208] [206]
- Evidence: IAM policy, MFA config screenshots, encryption configs, redaction unit tests, logging config, BAAs.
- Owner: Security Lead.
- Target Residual: Medium.
- Monitoring: SIEM alert on PHI regex in logs; weekly audit review; DLP failure ≥1 event triggers incident workflow.
- POA&M: POA&M-01.

R-02 Unsafe clinical statements (hallucinations)

- RMF: Select/Implement/Assess/Authorize/Monitor.[205]
- Description: Model generates incorrect/unsupported clinical content.
- Threat: Model limitations; adversarial prompts.
- Vulnerability: Lack of grounding checks; no clinician sign-off.
- Impact: High | Likelihood: Medium | Inherent: High.
- Assets/Data: Generation service, prompts, outputs.
- HIPAA: Integrity, Person/Entity Authentication; Admin—Workforce Security (human oversight).[206]
- 800-53: SA-11 (testing/verification), RA-5, SI-4 (monitoring), IR-4 (response), PL-2, SR-11 (model provenance).[207]
- Existing: Basic QA.
- Gaps: No groundedness threshold; no blocklists; no sign-off.
- Mitigation: Require retrieval-grounded generation; enforce groundedness ≥0.85 and ≤5% unsupported claims; clinician-in-the-loop sign-off before EHR post; medication/dose change

guardrails; red-team tests; document eval in SAR.[208]

- Evidence: Eval reports, blocked term lists, sign-off workflow SOP.
- Owner: Product + Clinical Safety.
- Residual: Medium.
- Monitoring: Alert if groundedness <0.85 or >1 unsupported claim/note average in rolling 100 notes; incident if safety-critical entity flagged.
- POA&M: POA&M-02.

R-03 Prompt injection/adversarial context

- RMF: Select/Implement/Assess/Monitor.[205]
- Description: Malicious text manipulates instructions to exfiltrate data or bypass policies.
- Threat: Crafted input in notes, external docs.
- Vulnerability: Unfiltered context; unrestricted tool behaviors.
- Impact: High | Likelihood: Medium | Inherent: High.
- HIPAA: Integrity, Access Control.[206]
- 800-53: SI-10 (input validation), SC-7 (boundary), SI-4, SR (supply chain).[207]
- Gaps: No sanitization; no allowlists.
- Mitigation: Sanitize inputs; strip/system-prompt isolation; allowlist instruction patterns; retrieval source whitelisting; adversarial test suite; monitoring for injection signatures.
- Evidence: Sanitization unit tests, WAF rules, test reports.
- Owner: Eng Lead.
- Residual: Medium.
- Monitoring: Detection of injection patterns ≥1/day triggers review.
- POA&M: POA&M-03.

R-04 Identity and access mismanagement

- RMF: Select/Implement/Assess/Monitor.[205]
- Description: Weak IAM allows unauthorized access.
- Threat: Credential theft; privilege creep.
- 800-53: AC-2/3/6, IA-2/5, AU-6, CM-5.[207]
- Mitigation: Central IAM, MFA, least privilege, quarterly access recerts, SoD.
- Evidence: IAM roles, recert logs.
- Residual: Low/Medium.
- Monitoring: Excess privilege alerts; failed MFA spikes.
- POA&M: POA&M-04.

R-05 Auditability and log integrity gaps

- RMF: Implement/Assess/Monitor.[205]
- 800-53: AU-2/3/6/8/9/12.[207]
- Mitigation: Immutable logs, time sync, retention policy, periodic review.
- Evidence: Log configs, review minutes.
- Residual: Low/Medium.
- Monitoring: Missed monthly reviews trigger escalation.
- POA&M: POA&M-05.

R-06 Data retention/minimization noncompliance

- RMF: Prepare/Categorize/Select/Implement/Monitor.[205]
- HIPAA: Admin/Technical safeguards; privacy considerations per 800-66.[206]
- 800-53: PL-2, MP family, AR/DM privacy controls (mapped via CPRT).[209] [207]
- Mitigation: Data inventory; retention schedule; purge jobs; consent/notice; de-identification before training.
- Evidence: Retention policy, purge logs.
- Residual: Medium.
- Monitoring: Purge job failures alert.
- POA&M: POA&M-06.

R-07 Third-party/vendor risk (BAAs, components)

- RMF: Select/Implement/Assess/Monitor.[205]
- Description: External services (speech-to-text, vector DB, hosting) mishandle ePHI.
- HIPAA: BAAs required; accountability retained by covered entity.[208]
- 800-53: SA-9 (external services), CA-3 (interconnections), SR-3/4, RA-3.[207]
- Mitigation: BAAs; vendor risk assessments; SBOMs; version pinning; CVE monitoring; interconnection agreements.
- Evidence: Signed BAAs, VRM reports.
- Residual: Medium.
- Monitoring: Quarterly vendor reviews; critical CVE alerts.
- POA&M: POA&M-07.

R-08 Model/data drift

- RMF: Assess/Monitor.[205]
- 800-53: CM-3 (change control), SI-4 (monitoring), PL-2 (eval cadence).[207]
- Mitigation: Drift dashboards; scheduled re-evals; rollback plan; A/B holdouts.
- Evidence: KPI dashboards, eval reports.
- Residual: Medium.

- Monitoring: Groundedness/time-in-notes KPI thresholds trigger rollback.
- POA&M: POA&M-08.

R-09 Incident response gaps (AI-specific)

- RMF: Implement/Assess/Authorize/Monitor.[205]
- 800-53: IR-4/5/6, CP-2.[207]
- Mitigation: AI-specific IR playbooks (PHI leakage, unsafe output, poisoning); HIPAA breach notification workflow; tabletop exercises.
- Evidence: IR plan, tabletop minutes.
- Residual: Medium.
- Monitoring: MTTA/MTTR SLO breaches escalate.
- POA&M: POA&M-09.

R-10 Availability/latency SLO breaches

- RMF: Implement/Assess/Monitor.[205]
- Description: Latency or downtime harms clinic flow and pushes after-hours work.
- 800-53: CP-10 (recovery), SC-5 (QoS), SI-4 (monitoring).[207]
- Mitigation: Capacity planning; autoscaling; circuit breakers; DR; fallbacks to manual templates; SLO dashboards.
- Evidence: Load test reports, DR test results.
- Residual: Medium.
- Monitoring: p95 > 60s or uptime < 99.5% triggers incident.
- POA&M: POA&M-10.

How to operate this register (as PM)

- Prepare: Define owners and cadence; link each risk to SSP sections and to POA&M tasks with due dates and measurable acceptance criteria.[209] [205]
- Assess and Authorize: Collect artifacts (configs, screenshots, BAAs, logs), compile SAR findings, and present residual risk to Authorizing Official for ATO decision; record accepted risks and compensating controls in this register.[205]
- Monitor: Review metrics monthly—groundedness ≥0.85, unsupported claims ≤5%/note, PHI leakage=0, uptime ≥99.5%, vendor reviews on schedule—and update statuses and POA&M closures accordingly.[208] [206]

Documentation pointers

- Use SP 800-66 Rev.2 official guide as primary reference for HIPAA alignment and sample activities/tables; keep a copy in the evidence folder.[206] [208]
- Use NIST Cybersecurity and Privacy Resource Tool (CPRT/OLIR) online mappings to link HIPAA safeguards to 800-53 controls for each risk/control row; note the mapping URL or export in Evidence column.[209] [207]

- Keep this register under version control with change history and periodic approvals by Security, Privacy, and Product leadership to demonstrate governance maturity.[208]

Citations

- NIST SP 800-66 Rev.2: Implementing HIPAA Security Rule (official guide, tables, mappings). [206] [208]
- NIST SP 800-37 Rev.2: RMF steps and artifacts for risk lifecycle and authorization.[205]
- NIST SP 800-53 Rev.5: Security and privacy control catalog for mapping safeguards.[209] [207]

⁂

explain how did you reference the framework for each risk and came up with risk register - tell me inmmost easiest languiage step by step process followed and explain all jargons, so that I can follow these steps for any other products

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.

2. 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.

3. 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.

4. 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).

5. 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).

6. 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.

7. 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).

8. 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.

9. 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.

If a single sentence is needed

- Start from how the product handles sensitive data, list concrete ways it could fail, map each to HIPAA safeguards and named NIST controls, write down practical fixes with owners and proof, then keep the list live with regular reviews and alerts.

⁂

1. https://ideausher.com/blog/build-hipaa-compliant-ai-healthcare-app/
2. https://blog.patientnotes.ai/2025/03/01/best-ai-clinical-documentation-tools-2025/
3. https://pmc.ncbi.nlm.nih.gov/articles/PMC9095342/
4. https://www.nuance.com/asset/en_uk/collateral/enterprise/report/rpt-assessing-the-burden-of-clinical-documentation-en-uk.pdf
5. https://amia.org/news-publications/amia-survey-underscores-impact-excessive-documentation-burden
6. https://pmc.ncbi.nlm.nih.gov/articles/PMC9936289/
7. https://www.omegahms.com/unlocking-enhanced-compliance-revenue-growth-with-ai-powered-cdi-solutions/
8. https://www.abridge.com
9. https://www.ncbi.nlm.nih.gov/books/NBK608542/
10. https://www.aapc.com/resources/what-is-clinical-documentation
11. https://www.heidihealth.com
12. https://www.sciencedirect.com/science/article/abs/pii/S1555415525001163
13. https://www.asha.org/practice-portal/professional-issues/documentation-in-health-care/
14. https://sunoh.ai
15. https://bmjopenquality.bmj.com/content/12/2/e002084
16. https://www.scphealth.com/blog/think-with-your-ink-4-reasons-why-proper-medical-record-documentation-is-vital/
17. https://www.suki.ai
18. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2837847
19. https://pmc.ncbi.nlm.nih.gov/articles/PMC11605373/
20. https://blogs.meditab.com/what-is-clinical-documentation-and-its-importanceyour-blog-post-title-here
21. https://compliancy-group.com/common-clinical-documentation-mistakes/

22. https://www.medicaleconomics.com/view/physicians-spend-4-5-hours-a-day-on-electronic-health-records
23. https://pubmed.ncbi.nlm.nih.gov/31931523/
24. https://www.ama-assn.org/practice-management/digital-health/five-physician-specialties-spend-most-time-ehr
25. https://www.ama-assn.org/practice-management/physician-health/measuring-and-addressing-physician-burnout
26. https://isass.org/report-finds-higher-rates-of-physician-burnout-in-recent-years/
27. https://www.aha.org/aha-center-health-innovation-market-scan/2024-07-16-work-remains-physician-burnout-rates-are-coming-down
28. https://www.advisory.com/daily-briefing/2024/07/15/physician-burnout
29. https://pmc.ncbi.nlm.nih.gov/articles/PMC7661623/
30. https://amia.org/news-publications/amia-survey-underscores-impact-excessive-documentation-burden
31. https://pmc.ncbi.nlm.nih.gov/articles/PMC8961402/
32. https://www.aha.org/guidesreports/2024-09-10-skyrocketing-hospital-administrative-costs-burdensome-commercial-insurer-policies-are-impacting
33. https://www.pgpf.org/article/almost-25-percent-of-healthcare-spending-is-considered-wasteful-heres-why/
34. https://med.stanford.edu/news/all-news/2025/04/doctor-burnout-rates-what-they-mean.html
35. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2833027
36. https://www.ama-assn.org/practice-management/digital-health/digging-data-cut-ehr-burdens-drive-burnout
37. https://www.ama-assn.org/practice-management/sustainability/3-ways-begin-reduce-clinical-documentation-75-2025
38. https://medinform.jmir.org/2024/1/e54811/
39. https://docit.ucsf.edu/news/new-study-shows-high-levels-ehr-documentation-burden-crowd-out-use-hie
40. https://pmc.ncbi.nlm.nih.gov/articles/PMC10134123/
41. https://academic.oup.com/jamia/article/28/5/998/6090156
42. https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2822382
43. https://pmc.ncbi.nlm.nih.gov/articles/PMC10734365/
44. https://www.ncbi.nlm.nih.gov/books/NBK608542/
45. https://www.ama-assn.org/practice-management/physician-health/doctors-work-fewer-hours-ehr-still-follows-them-home
46. https://www.sciencedirect.com/science/article/pii/S0025619624000375
47. https://www.sciencedirect.com/science/article/abs/pii/S1555415525001163
48. https://academic.oup.com/jamia/article/32/1/235/7824350
49. https://connectwithcare.org/wp-content/uploads/2024/04/jamainternal_holmgren_2023_oi_230072_1702335740.03218.pdf
50. https://www.healthit.gov/sites/default/files/2024-01/Exploring-the-Relationship-between-Payment-Models-and-Documentation-Burden_508.pdf

51. https://pubmed.ncbi.nlm.nih.gov/37902737/
52. https://sma.org/ama-reports-physician-burnout-rate-falls-below-50/
53. https://pmc.ncbi.nlm.nih.gov/articles/PMC11918610/
54. https://www.kff.org/health-costs/americans-challenges-with-health-care-costs/
55. https://www.urologytimes.com/view/analysis-highlights-gender-gap-in-physician-time-spent-on-ehr-and-documentation
56. https://www.ama-assn.org/about/ama-research/trends-health-care-spending
57. https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2830185
58. https://www.ama-assn.org/practice-management/physician-health/national-physician-burnout-study-latest-statistics-burnout
59. https://pmc.ncbi.nlm.nih.gov/articles/PMC12059965/
60. https://developer.nvidia.com/blog/evaluating-medical-rag-with-nvidia-ai-endpoints-and-ragas/
61. https://pmc.ncbi.nlm.nih.gov/articles/PMC10635391/
62. https://www.jmir.org/2025/1/e68998
63. https://galileo.ai/blog/mastering-rag-improve-performance-with-4-powerful-metrics
64. https://www.nature.com/articles/s41598-024-84850-x
65. https://www.simbo.ai/blog/addressing-the-gaps-in-ambient-scribe-evaluation-the-need-for-standardized-metrics-and-diverse-clinical-specialty-considerations-3616268/
66. https://pmc.ncbi.nlm.nih.gov/articles/PMC11840636/
67. https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2830185
68. https://www.nature.com/articles/s41746-025-01622-1
69. https://www.sciencedirect.com/science/article/pii/S1386505625003302
70. https://www.evidentlyai.com/llm-guide/rag-evaluation
71. https://www.sciencedirect.com/science/article/pii/S1532046424000807
72. https://www.acceldata.io/blog/how-rag-in-ai-is-transforming-conversational-ai
73. https://hatchworks.com/blog/gen-ai/rag-for-healthcare/
74. https://sarahgebauermd.substack.com/p/measuring-what-matters-the-ambient
75. https://www.deepscribe.ai/resources/deepscore-measuring-the-performance-of-ambient-ai-clinical-documentation
76. https://www.nature.com/articles/s43856-025-01091-3
77. https://pmc.ncbi.nlm.nih.gov/articles/PMC8367121/
78. https://web.stanford.edu/class/cs224n/final-reports/256989380.pdf
79. https://pmc.ncbi.nlm.nih.gov/articles/PMC12316405/
80. https://www.evidentlyai.com/llm-guide/rag-evaluation
81. https://developer.nvidia.com/blog/evaluating-medical-rag-with-nvidia-ai-endpoints-and-ragas/
82. https://www.deepset.ai/blog/rag-llm-evaluation-groundedness
83. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2833433
84. https://pmc.ncbi.nlm.nih.gov/articles/PMC12048851/
85. https://pmc.ncbi.nlm.nih.gov/articles/PMC11840636/

86. https://www.nature.com/articles/s41598-024-84850-x
87. https://www.jmir.org/2025/1/e68998
88. https://pmc.ncbi.nlm.nih.gov/articles/PMC10635391/
89. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2837847
90. https://www.massgeneralbrigham.org/en/about/newsroom/press-releases/ambient-documentation-technologies-reduce-physician-burnout
91. https://www.ama-assn.org/practice-management/digital-health/ai-scribes-save-15000-hours-and-restore-human-side-medicine
92. https://sporevidencealliance.ca/wp-content/uploads/2024/11/SPOREA_AI_SCRIBE_FINAL_Report.pdf
93. https://pmc.ncbi.nlm.nih.gov/articles/PMC12166074/
94. https://www.nature.com/articles/s41746-025-01622-1
95. https://pmc.ncbi.nlm.nih.gov/articles/PMC12059965/
96. https://pmc.ncbi.nlm.nih.gov/articles/PMC12193156/
97. https://amplifycare.com/resource/cutting-the-after-hours-how-ai-scribes-are-giving-clinicians-their-time-back/
98. https://www.nature.com/articles/s41746-025-01895-6
99. https://himcos.com/metrics-to-measure-efficiency-of-ai-medical-scribe/
100. https://www.qed42.com/insights/simplifying-rag-evaluation-with-ragas
101. https://medinform.jmir.org/2025/1/e80898
102. https://www.ai21.com/knowledge/rag-evaluation/
103. https://www.thieme-connect.de/products/ejournals/pdf/10.1055/a-2597-2017.pdf
104. https://news.harvard.edu/gazette/story/2025/08/physicians-embrace-ai-note-taking-technology/
105. https://agenta.ai/blog/how-to-evaluate-rag-metrics-evals-and-best-practices
106. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2833433
107. https://medicalxpress.com/news/2025-05-ambient-ai-technology-documentation-burden.html
108. https://www.beckershospitalreview.com/healthcare-information-technology/ehrs/where-mass-general-brigham-is-taking-its-ambient-documentation-efforts-next/
109. https://www.massgeneralbrigham.org/en/about/newsroom/press-releases/ambient-documentation-technologies-reduce-physician-burnout
110. https://news.harvard.edu/gazette/story/2025/08/physicians-embrace-ai-note-taking-technology/
111. https://medicalxpress.com/news/2025-08-ambient-documentation-technologies-physician-burnout.html
112. https://pmc.ncbi.nlm.nih.gov/articles/PMC12166074/
113. https://pmc.ncbi.nlm.nih.gov/articles/PMC12059965/
114. https://developer.nvidia.com/blog/evaluating-medical-rag-with-nvidia-ai-endpoints-and-ragas/
115. https://arxiv.org/html/2411.09213v1
116. https://aclanthology.org/2024.findings-acl.372.pdf
117. https://www.ama-assn.org/practice-management/digital-health/ai-scribes-save-15000-hours-and-restore-human-side-medicine
118. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2830383

119. https://pubmed.ncbi.nlm.nih.gov/40314951/
120. https://pubmed.ncbi.nlm.nih.gov/40694347/
121. https://academic.oup.com/jamia/article/32/4/605/7954485
122. https://www.imohealth.com/resources/improving-ambient-ai-accuracy-with-a-clinical-foundation/
123. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2837847
124. https://teddy-xionggz.github.io/benchmark-medical-rag/
125. https://www.gastroenterologyadvisor.com/news/ambient-documentation-technology-helps-to-reduce-clinician-burnout/
126. https://www.news-medical.net/news/20250222/AI-scribe-technology-decreases-documentation-burden-for-clinicians.aspx
127. https://www.massgeneralbrigham.org/en/about/newsroom
128. https://www.louisbouchard.ai/rag-evals/
129. https://pmc.ncbi.nlm.nih.gov/articles/PMC12059965/
130. https://aclanthology.org/2024.findings-acl.372.pdf
131. https://arxiv.org/html/2402.13178v1
132. https://developer.nvidia.com/blog/evaluating-medical-rag-with-nvidia-ai-endpoints-and-ragas/
133. https://www.evidentlyai.com/llm-guide/rag-evaluation
134. https://toloka.ai/blog/rag-evaluation-a-technical-guide-to-measuring-retrieval-augmented-generation/
135. https://qdrant.tech/blog/rag-evaluation-guide/
136. https://arxiv.org/html/2411.09213v1
137. https://intuitionlabs.ai/articles/rag-performance-pharmaceutical-documents
138. https://www.promptingguide.ai/research/rag
139. https://teddy-xionggz.github.io/benchmark-medical-rag/
140. https://arxiv.org/html/2405.07437v2
141. https://www.nature.com/articles/s41598-025-00724-w
142. https://labelyourdata.com/articles/llm-fine-tuning/rag-evaluation
143. https://csrc.nist.gov/pubs/sp/800/37/r2/final
144. https://www.device42.com/compliance-controls/nist-800-37/
145. https://www.island.io/content/compliance/nist-800-37
146. https://hyperproof.io/nist-800-53/
147. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
148. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
149. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf
150. https://anchore.com/compliance/nist/800-53/
151. https://www.securityscientist.net/blog/a-guide-to-the-nist-risk-management-framework-nist-sp-800-37/
152. https://www.eccouncil.org/cybersecurity-exchange/incident-handling/nist-risk-management-framework-rmf-guide/
153. https://sprinto.com/blog/nist-risk-management-framework/

154. https://www.vanta.com/resources/nist-ai-risk-management-framework
155. https://www.leonardodrs.com/wp-content/uploads/2023/08/cs3-rmfp-template.pdf
156. https://www.metricstream.com/learn/nist-sp-800-53.html
157. https://www.scrut.io/post/step-by-step-guide-to-apply-rmf
158. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
159. https://anchore.com/compliance/nist/800-37/
160. https://www.censinet.com/perspectives/nist-csf-and-hipaa-crosswalk-explained
161. https://www.neotas.com/risk-management-framework/
162. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
163. https://csrc.nist.gov/pubs/sp/800/66/r2/final
164. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
165. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
166. https://csrc.nist.gov/pubs/sp/800/37/r2/final
167. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
168. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
169. https://www.paubox.com/blog/updated-guidance-overview-nist-800-66-rev2
170. https://www.hipaasecurenow.com/nist-and-hipaa/
171. https://csrc.nist.gov/pubs/sp/800/66/r2/ipd
172. https://www.meditologyservices.com/unveiling-the-updates-navigating-nist-sp-800-66-rev-2/
173. https://continuumgrc.com/audit-compliance-solutions-hipaa/
174. https://www.scirp.org/journal/paperinformation?paperid=132826
175. https://www.linkedin.com/pulse/its-here-nist-special-publication-sp-800-66-revision-2-richardson-taomc
176. https://mitratech.com/resource-hub/blog/nist-800-66/
177. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf
178. https://csrc.nist.gov/pubs/sp/800/66/r2/final
179. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
180. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
181. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
182. https://continuumgrc.com/audit-compliance-solutions-hipaa/
183. https://csrc.nist.gov/pubs/sp/800/37/r2/final
184. https://www.scirp.org/journal/paperinformation?paperid=132826
185. https://www.bartonassociates.com/locum-tenens-resources/hipaa-compliance-quiz/
186. https://www.saltycloud.com/blog/hipaa-security-rule/
187. https://www.easyllama.com/blog/hipaa-questions
188. https://calibr.ai/blogs/hipaa-quiz-answers
189. https://www.med.upenn.edu/hipaa/attach/DRAFT-sp800-66.pdf
190. https://csrc.nist.gov/pubs/sp/800/66/r2/final
191. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

192. https://www.pyapc.com/insights/5-key-takeaways-for-hipaa-cybersecurity-from-nist-special-publication/
193. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
194. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
195. https://csrc.nist.rip/News/2024/nist-publishes-sp-80066-revision-2-implementing-th
196. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
197. https://www.scirp.org/journal/paperinformation?paperid=132826
198. https://www.pivotpointsecurity.com/nist-update-on-hipaa-security-rule-can-help-your-org-reduce-ephi-risk-exposure/
199. https://www.meditologyservices.com/unveiling-the-updates-navigating-nist-sp-800-66-rev-2/
200. https://download.manageengine.com/active-directory-360/ebooks/nist-800-66-controls-to-achieve-hipaa-compliance.pdf
201. https://csrc.nist.rip/publications/detail/sp/800-66/rev-2/draft
202. https://www.compliancepoint.com/healthcare/nist-updates-impact-hipaa-security-rule/
203. https://www.paubox.com/blog/updated-guidance-overview-nist-800-66-rev2
204. https://mitratech.com/resource-hub/blog/nist-800-66/
205. https://csrc.nist.gov/pubs/sp/800/37/r2/final
206. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf
207. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
208. https://csrc.nist.gov/pubs/sp/800/66/r2/final
209. https://csrc.nist.rip/News/2024/nist-publishes-sp-80066-revision-2-implementing-th
210. https://continuumgrc.com/audit-compliance-solutions-hipaa/
211. https://www.eccouncil.org/cybersecurity-exchange/incident-handling/nist-risk-management-framework-rmf-guide/
212. https://www.cloudauditcontrols.com/2022/09/hippa-nist-updated-guidance-for-health.html
213. https://regscale.com/blog/understanding-nist-rmf/
214. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf
215. https://www.neotas.com/risk-management-framework/
216. https://ecfirst.com/pdf/NIST_References.pdf
217. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
218. https://www.sailpoint.com/identity-library/nist-risk-management-framework
219. https://www.securityscientist.net/blog/a-guide-to-the-nist-risk-management-framework-nist-sp-800-37/
220. https://cybersierra.co/blog/nist-risk-management-framework-the-complete-guide/
221. https://anchore.com/compliance/nist/800-37/
222. https://www.scirp.org/journal/paperinformation?paperid=132826
223. https://www.compliancepoint.com/healthcare/nist-updates-impact-hipaa-security-rule/
224. https://www.paubox.com/blog/updated-guidance-overview-nist-800-66-rev2
225. https://www.device42.com/compliance-controls/nist-800-37/

226. https://www.eccouncil.org/cybersecurity-exchange/incident-handling/nist-risk-management-framework-rmf-guide/
227. https://csrc.nist.gov/projects/risk-management/about-rmf/prepare-step
228. https://www.scrut.io/post/how-to-create-a-risk-register
229. https://www.centraleyes.com/nist-risk-assessment-template-a-step-by-step-guide-to-effective-risk-management/
230. https://regscale.com/blog/understanding-nist-rmf/
231. https://cybersierra.co/blog/nist-risk-management-framework-the-complete-guide/
232. https://www.cdse.edu/Portals/124/Documents/student-guides/CS101-guide.pdf
233. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
234. https://www.cloudeagle.ai/blogs/risk-management-framework-a-step-by-step-guide-for-it-leaders