

Healthcare Practice Safety Check

Patient-data safety & AI · Revenue cycle health

Fareez Mamood, RN · Engineering intelligent solutions to wellbeing

Do not write patient information on this sheet. Answer for the practice as a whole.

Part A · Patient-data safety & AI

	Yes 2	Partly 1	No/unsure 0
1 Do you know which AI tools your staff already use, including free chatbots on phones? Next step: Make a one-page list of every AI tool in use before adding anything new.	☐	☐	☐
2 Is there a written rule that patient information never goes into a tool without a signed business associate agreement (BAA)? Next step: Write a one-line rule: no patient information in any tool without a signed BAA, and tell every staff member.	☐	☐	☐
3 Do the vendors that already handle your patient data have signed BAAs on file? Next step: Collect and file the BAAs for every vendor that touches patient data.	☐	☐	☐
4 Do you know every place patient information is stored or sent, including cloud storage, texting, email, fax and any AI or transcription tool? Next step: Draw a one-page map of where patient information lives and travels, including any outside servers.	☐	☐	☐
5 Is there a written procedure for releasing patient records (who approves, how the requester is verified, and sending only the minimum needed)? Next step: Write a one-page release procedure: who approves, how the requester is verified, and only the records needed go out.	☐	☐	☐
6 Before records go out by fax, email or portal, does a second check confirm the recipient and the contents? Next step: Add a two-point check before any release: the right person, and only the right records.	☐	☐	☐
7 Is there a written plan for a suspected impermissible disclosure, with one named person who decides what happens next? Next step: Write a one-page incident plan and name the person staff report to right away. Patient notice is due without unreasonable delay and within 60 days of discovery.	☐	☐	☐
8 Can you name your top three time drains (e.g. prior auth, documentation, phones, denials)? Next step: Pick the top three time drains with your team. AI only helps where the work is measured.	☐	☐	☐
9 Do you know what your EHR vendor offers for electronic prior auth or other integrations? Next step: Ask your EHR vendor what electronic prior-auth (FHIR) support is on their roadmap for 2027.	☐	☐	☐
10 Is one named person responsible for evaluating new technology or AI tools? Next step: Name one person who owns tool decisions, even for a few hours a month.	☐	☐	☐
11 Does a clinician review every AI-drafted note, letter or appeal before it is used? Next step: Make human review of every AI draft a rule, and write it down.	☐	☐	☐
12 Have staff been shown how AI tools can be confidently wrong? Next step: Run a short team session with real examples of AI mistakes.	☐	☐	☐

Part B · Revenue cycle health

	Yes 2	Partly 1	No/unsure 0
13 Do you know your first-pass (clean) claim rate? Next step: Track your clean claim rate monthly; it is the earliest warning sign.	☐	☐	☐
14 Do you know your denial rate and your top denial reasons? Next step: Group last quarter's denials by reason.	☐	☐	☐
15 Do you know your days in accounts receivable (A/R)? Next step: Review days in A/R monthly, by payer.	☐	☐	☐
16 Do you track how many prior authorizations you submit each week and how long they take? Next step: Start a simple weekly count of prior auths and days to decision.	☐	☐	☐
17 Do you know which payers require prior auth for your 10 most common services? Next step: Keep a one-page payer matrix for your most common services.	☐	☐	☐
18 Do you verify eligibility and benefits before every visit? Next step: Check eligibility and benefits before the visit, not after the denial.	☐	☐	☐
19 Is your coding reviewed by someone independent at least once a year, for both under- and over-coding? Next step: Run an annual sample audit for coding accuracy in both directions.	☐	☐	☐
20 Do you check payments against your contracted rates and track appeal outcomes? Next step: Flag underpayments against your contracts, and track which appeals you win.	☐	☐	☐
21 Do coders or billers feed documentation gaps back to providers? Next step: Set up a short monthly documentation feedback loop between billing and providers.	☐	☐	☐

Part A: ____ / 24

20-24 Strong
11-19 Building
0-10 Start with the basics

Part B: ____ / 18

15-18 Strong
9-14 Building
0-8 Start with the basics

Total: ____ / 42

Work first on the "Next step" lines where you scored 0 or 1.

Reference: patient-data safety and prior auth

Patient-data safety: where practices get into trouble

Three common ways patient information gets exposed. Sources are the HIPAA rules (45 CFR Part 164) and HHS Office for Civil Rights guidance.

Patient information going to outside servers

Pasting notes into a free or personal AI chatbot, or using an AI, transcription, cloud-storage, texting or email tool for patient information. If an outside vendor creates, receives, stores or sends patient information for you, HIPAA generally requires a signed business associate agreement (BAA) first. Cloud services that store patient information count as business associates even when the data is encrypted and they do not hold the key. Check each vendor's terms for a signed BAA before any patient information goes in. 45 CFR 164.502(e), 164.504(e); HHS OCR, Guidance on HIPAA & Cloud Computing

Records released to the wrong place or in the wrong amount

Sending records to the wrong fax number, email address or person, releasing without a valid patient authorization when one is needed, or sending more than the minimum necessary. Each can be an impermissible disclosure. 45 CFR 164.502(a), 164.502(b), 164.508(a)

What happens after a mistake

An impermissible disclosure is presumed to be a breach unless a documented risk assessment shows a low probability that the information was compromised. Affected patients must be told without unreasonable delay and no later than 60 calendar days after discovery, and HHS must be notified. HHS can impose civil money penalties for violations. 45 CFR 164.402, 164.404(b), 164.408, 160.404

Rules: [ecfr.gov](https://www.ecfr.gov), Title 45 Part 164. Guidance: [hhs.gov/hipaa](https://www.hhs.gov/hipaa). Education only, not legal advice; this page does not tell you whether your practice is or is not in compliance.

Prior auth & denials: 2026-2027 quick reference

From the CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F, 89 FR 8758, Feb 8, 2024).

Which plans

Medicare Advantage; Medicaid and CHIP (fee-for-service and managed care); qualified health plans on the federal Exchanges (HealthCare.gov). Commercial and employer plans are not covered. 89 FR 8759, 8760

Decision deadlines (from 2026)

Medicare Advantage, Medicaid and CHIP: 72 hours for expedited, 7 calendar days for standard requests. Federal-Exchange plans keep their existing deadlines. 42 CFR 422.568(b)(1), 440.230(e)(1), 438.210(d), 457.495(d)

Denials must say why (from 2026)

A denied prior-auth request must come with a specific reason: Medicare Advantage, Medicaid (fee-for-service and managed care), CHIP fee-for-service and federal-Exchange plans. 42 CFR 422.122(a), 431.80(a), 438.242(b)(8), 457.732(a); 45 CFR 156.223(a)

Public metrics (from 2026)

Payers publish prior-auth data (drugs excluded) every year by March 31. 42 CFR 422.122(c); 45 CFR 156.223(c)

Electronic prior auth (from 2027)

Payers must offer a Prior Authorization API (FHIR). It shows whether auth is needed and what documentation to send, and it accepts requests electronically. Start dates run from Jan 1, 2027 or from the first plan/rating year after it. 42 CFR 422.122(b), 431.80(b), 457.732(b); 45 CFR 156.223(b)

For clinicians and hospitals (2027)

A new yes/no "Electronic Prior Authorization" measure starts in MIPS Promoting Interoperability and the Medicare Promoting Interoperability Program. 89 FR 8758, section II.F

Drugs are excluded

None of the above applies to drugs of any kind, including pharmacy and medical-benefit drugs. Drug prior auth follows separate rules. 89 FR 8762; 42 CFR 422.119(b)(1)(v); 45 CFR 156.221(b)(1)(v)

Rule text: [federalregister.gov](https://www.federalregister.gov), document 2024-00895; current regulations at [ecfr.gov](https://www.ecfr.gov).



Fareez Mamood, RN · Engineering intelligent solutions to wellbeing
954-681-7308 · fareez@synlearns.ai
Online version: aicheck.synlearns.ai

Education only, not legal or billing advice. Check your payer contracts and the cited rule text for your situation.