

HIPAA and AI: five questions a clinic should ask before switching anything on

An AI demo can look helpful long before the workflow is ready for patient information. Start with these five questions.

IN THIS GUIDE

- | | |
|--|---|
| 1. What information enters the system, and where does it go? | 4. Who checks the output before it affects a patient? |
| 2. Are the right agreements in place for this exact use? | 5. What happens if the tool fails—or you stop using it? |
| 3. Who can access the information, and how is access controlled? | Before switching it on |

An AI note-taking tool produces a convincing summary. A chatbot answers a patient question. A new button promises to turn intake forms into a care-plan draft.

The demonstration is the easy part. Before enabling the feature, a clinic needs to understand what happens to patient information—and who is responsible when something goes wrong.

For clinics subject to HIPAA, the existing privacy and security obligations still apply when a vendor uses AI. HHS requires administrative, physical, and technical safeguards for electronic protected health information, or ePHI.^[3] A feature being useful does not establish that it is appropriate for your practice.

Use these five questions to turn a sales conversation into a deployment decision.

1. What information enters the system, and where does it go?

Ask for a data-flow diagram, not just a statement that the product is secure. Trace the information from collection through processing, storage, and deletion.

Include audio recordings, transcripts, uploaded files, prompts, generated responses, support access, backups, and diagnostic logs. Ask whether another company supplies transcription, the AI model, or document storage.

Then ask what happens to that information after the response appears. Can it be used for model training, product improvement, or human review? What retention settings actually apply to your account and feature?

A useful answer: A written explanation of the complete workflow, the organizations involved, permitted uses, and retention periods.

Do not assume removing a patient's name makes a note de-identified. HIPAA recognizes specific Expert Determination and Safe Harbor methods; simply deleting a name does not establish that either method has been satisfied.^[2]

2. Are the right agreements in place for this exact use?

When a cloud provider creates, receives, maintains, or transmits ePHI on a covered entity's behalf, HHS generally treats it as a business associate and requires a HIPAA-compliant business associate agreement, or BAA—even when it cannot decrypt the information.^[1]

Ask whether the agreement covers the particular product, subscription, feature, and integration you intend to enable. A BAA for one service should not be assumed to cover every service bearing the same logo.

Also ask how the vendor handles subcontractors. A business associate must obtain appropriate contractual assurances from subcontractors handling ePHI on its behalf.^[3]

A useful answer: An applicable agreement and a clear division of responsibilities—not a marketing badge. A BAA does not replace your clinic's risk analysis or the other HIPAA requirements.^[1]

3. Who can access the information, and how is access controlled?

HHS calls for risk analysis and safeguards appropriate to the organization and its risks; encryption alone does not address every requirement.^{[1][3]}

As practical implementation checks, ask about individual accounts, role-based permissions, multifactor authentication, device security, audit logs, and offboarding. Who can export records? Can a vendor support technician see patient information? Who approves and reviews that access?

Include the surrounding workflow. A carefully configured AI service does little to help if staff paste its output into an unauthorized personal account.

A useful answer: Documented controls, named owners, and a demonstration that access restrictions work. Include the new workflow in the clinic's security risk analysis before introducing patient data.

4. Who checks the output before it affects a patient?

Privacy and clinical suitability are separate decisions. A signed agreement tells you nothing about whether a generated summary omitted an allergy or a suggested code fits the documented service.

For an initial clinical rollout, require a qualified reviewer to compare the output with its source before it enters the record or influences care. Make drafts visibly identifiable. Define which tasks the tool may perform and which it must not perform.

Test realistic failure scenarios: missing information, conflicting medications, ambiguous dictation, and an incorrect patient match. These are recommended clinical-safety checks, not a claim that HIPAA itself prescribes a particular AI review process.

A useful answer: A named clinical owner, an approval step, and documented criteria for acceptable performance—not “the clinician can edit it.”

5. What happens if the tool fails—or you stop using it?

Ask how staff continue working during an outage, how records are recovered, how access is revoked, and how information is exported or deleted at contract end. HHS identifies availability, recovery, data return, and retention limitations as relevant issues in cloud-service agreements.^[1]

Define the incident escalation path with your privacy and security leads. Business associates have reporting obligations for security incidents and breaches under the applicable rules and agreements.^[3] Do not leave responsibilities or reporting timelines to an assumption made during an emergency.

A useful answer: A tested fallback, an exit plan, and named contacts on both sides.

Before switching it on

- ☐ Approve a specific use case and identify its owner.
- ☐ Map the data flow and review applicable agreements.
- ☐ Complete the relevant privacy and security assessment.
- ☐ Test access controls, output review, and failure handling.
- ☐ Train staff on approved use and prohibited inputs.
- ☐ Start with synthetic examples, then permit patient data only after the required review and approvals.

Bottom line: Adopt a defined, reviewed workflow—not an AI feature in isolation.

Considering an AI tool for your clinic? Start with a workflow review alongside your privacy, security, and clinical leads before committing to a rollout.

This guide provides general educational information, not legal or clinical advice. Have qualified counsel and your compliance team assess the specific use, including other applicable privacy, recording, and medical-device requirements.

Sources

[1] <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>

[2] <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>

[3] <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>