

TWELVE QUESTION SELF ASSESSMENT

Twelve questions your board should be able to answer.

Answer these standing up, in about four minutes. Count every answer that is not a confident yes, because a surveyor, an insurer, and a state attorney general all treat not sure the way they treat no.

START HERE. CHECK THE BOX THAT DESCRIBES YOUR CLINIC.

- ☐ **Path A.** We bill Medicaid or private insurance.
You are a HIPAA covered entity. Answer the A wording where it appears.
- ☐ **Path B.** We do not bill insurance.
You are generally not a covered entity, and you hold real duties anyway. Answer the B wording.

	YES	NO	NOT SURE
1 Could you prove, line by line, every privacy claim your website and intake forms already make? A Including the patient right to complain to the Secretary of Health and Human Services. B Including that you describe voluntary alignment and never claim to be HIPAA compliant.	☐	☐	☐
2 Do you know what patient information sits on each ultrasound machine, and on anything plugged into it?	☐	☐	☐
3 Is every external drive attached to a clinical device blocked from the computers at your front desk?	☐	☐	☐
4 Can you show that storage on your ultrasound machines is encrypted, and not only password protected?	☐	☐	☐
5 If ransomware locked your systems tonight, could you name the backup you would restore from, and the date someone last proved it works by restoring an actual file?	☐	☐	☐
6 Do you hold a written list of every artificial intelligence tool in use, including the features built into software you already pay for?	☐	☐	☐
7 If a staff member pasted patient information into a public AI tool last month, would you know?	☐	☐	☐
8 When a scribe or transcription tool drafts a clinical note, can you open a chart today and show where a qualified professional verified it and signed as the author?	☐	☐	☐
9 For every vendor that can reach patient information, do you hold a signed agreement requiring them to notify you of a breach within a set number of days? A A business associate agreement. B A confidentiality and data protection agreement that also bars training on your data.	☐	☐	☐
10 When a patient raises a privacy concern, who receives it by name, and how many days do they have to respond in writing? A Your Privacy Officer, and patients are told they may also complain to Health and Human Services. B Your Privacy Officer, under your grievance process, with no claim that a federal pathway exists.	☐	☐	☐
11 In the last year, have you run one drill where the record system was down and the ultrasound was unavailable at the same time?	☐	☐	☐
12 Does your governing body receive a written technology and clinical risk report, and does it appear in the minutes?	☐	☐	☐

COUNT YOUR NO AND NOT SURE ANSWERS

0 to 2

Ahead of most clinics we assess. Your work is holding that position through the accreditation cycle and having it verified from outside.

3 to 6

The common range. Every item is a finding waiting for a survey, an audit, or a bad Tuesday. Start with your not sure answers.

7 or more

Begin with three documents, your written regulatory status, your AI tool inventory, and your device and storage inventory.

Why the first question comes first. A clinic that does not bill insurance is generally not a HIPAA covered entity, and voluntarily meeting HIPAA grade standards is good stewardship. The exposure sits in the label, because recent attorney general complaints rested on state unfair and deceptive practices statutes, which reach nonprofits. Say that you voluntarily align with the standards of the HIPAA Security Rule where you can prove it, and retire the phrase HIPAA compliant.

Leave this page with us and we will tell you which three to fix first.

No obligation, and if we are not the right fit we will say so and point you somewhere useful.

austinzierke.com/consultation • hello@austinzierke.com

NAME _____	POSITION _____	ORGANIZATION _____
EMAIL _____	PHONE _____	