Top 5 Objections to a HIPAA Risk Analysis

Honest answers, for small healthcare practice owners weighing the investment

1. "WE ALREADY USE COMPLIANCY GROUP, HIPAA SECURE NOW, OR ACCOUNTABLE HQ."

That software covers training delivery, BAA storage, and document templates. It does not produce a written Risk Analysis that OCR will accept.

In every OCR settlement in the first four months of 2026 where the practice had compliance software on file, OCR still cited the missing or inadequate Risk Analysis as the primary deficiency. The software dashboard is internal-facing; an OCR audit requires auditor-facing documentation. They are different artifacts produced for different audiences.

The software tells you whether your training is current. OCR asks whether your Risk Analysis identifies every system containing electronic PHI, scores each risk by likelihood and impact, and documents remediation. No compliance software on the market today produces that output.

2. "We're too small for OCR to care."

OCR settled six HIPAA cases in the first four months of 2026, collecting over $1.28 million. The Right of Access Initiative has now produced more than 50 enforcement actions. The most recent against a solo dentist who charged a patient a $25 flat fee for medical records resulted in a $70,000 settlement.

The 2017 HHS audit found that fewer than 14 percent of covered entities substantially met Risk Analysis requirements, meaning the other 86 percent are out of compliance regardless of size. HIPAA applies uniformly to all covered entities, from solo practices to hospital systems. Size is not a defense.

3. "The cost is too high."

The lowest OCR Risk Analysis settlement on record in 2026 was $35,000, roughly ten times the cost of a properly conducted Risk Analysis. The average settlement runs closer to $150,000 plus a 2-to-3-year Corrective Action Plan that requires quarterly OCR reporting and consumes significant staff time.

The investment in a Risk Analysis is not the question. The question is whether you would rather pay $4,000 now to a CIPP/US certified professional or $150,000 later to OCR. Both are real costs. Only one is preventable.

4. "We had a consultant do this 2 or 3 years ago."

OCR's audit protocol explicitly requires Risk Analysis updates whenever the practice changes, new systems, new staff, new vendors, new locations, new service lines. HHS Final Guidance treats Risk Analysis as an ongoing requirement, with most practices needing at least annual updates.

A 3-year-old document is treated by OCR as no document. They have cited stale Risk Analysis as a deficiency in enforcement actions as recently as 2026. Settled case files specifically note when a practice "had previously conducted a Risk Analysis" but failed to update it to reflect current operations.

5. "Our IT vendor handles HIPAA."

Your IT vendor handles network security. That covers roughly 30 percent of the HIPAA Security Rule, the Technical Safeguards portion. The other 70 percent is the practice's direct responsibility: Administrative Safeguards (workforce training, sanction policies, contingency planning, BAA management), Physical Safeguards (facility access, workstation security, device controls), and the Privacy Rule and Breach Notification Rule entirely.

Your IT vendor's BAA explicitly excludes that work. The contract proves it. If you have not read your IT vendor's BAA in the last 12 months, that is the first place to look.

WHAT "DOING IT RIGHT" ACTUALLY MEANS

A defensible HIPAA Risk Analysis is:

- Written. Not a software dashboard or a checklist.
- Comprehensive. Covers every system containing electronic PHI.
- Risk-scored. Likelihood and impact rated for every identified threat.
- Documented remediation. Every Medium or High risk has an assigned action and owner.
- Signed and dated. By the practice owner or Privacy Officer.
- Updated at least annually, plus whenever operations materially change.

Built against the nine elements of HHS Final Guidance and the five criteria of HHS Audit Protocol. Mapped to NIST SP 800-30. Three weeks from start to delivery.

Sam Cherkaoui, CIPP/US | sam@northprivacyadvisors.com | (713) 925-9929