What OCR Actually Checks in a HIPAA Risk Analysis

The documents to have ready before a letter ever arrives.
Written for small healthcare practice owners.

WHY THE RISK ANALYSIS COMES FIRST

When OCR opens a HIPAA investigation, the first document it asks for is almost always your written Risk Analysis, required under **45 CFR 164.308(a)(1)(ii)(A).** It is the foundation of the Security Rule. Every other safeguard, policy, and corrective step is supposed to flow from it.

It is also the single most common failure. In OCR's recent years HIPAA Audits Industry Report, **86% of covered entities did not meet expectations for risk analysis.** Fewer than one in seven had one that held up.

Source: HHS OCR, 2016–2017 HIPAA Audits Industry Report.

THE FOUR THINGS OCR CHECKS FOR

In settled enforcement cases, OCR keeps citing the same four gaps. An investigator is checking whether:

- A Risk Analysis **exists at all**, in writing, signed and dated.
- It covers **every system** that creates, receives, stores, or transmits ePHI, not just the EHR.
- It is **current.** A Risk Analysis last updated more than two years ago is treated as no analysis.
- Identified risks were **actually remediated**, with the corrective steps documented.

The investigator wants proof you knew what your risks were and that you addressed them. A software dashboard or a compliance "seal" is not a substitute for the analysis itself.

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

WHAT YOU SHOULD HAVE READY

Five documents make up the core of an OCR response. The Risk Analysis is the spine; the rest reference it.

- A written **Risk Analysis dated within the last 12 months**, signed by the owner or Privacy Officer.
- A signed **BAA on file with every vendor** that touches PHI.
- **Workforce HIPAA training records** for the current calendar year.
- A written **breach response plan**, including the 60-day notification procedure.
- **Documentation of remediation** for any risk rated Medium or higher.

WHAT'S ACTUALLY AT STAKE

Civil penalties under HIPAA in 2026 run from **$145 per violation** (Tier 1: Did Not Know) to **$2,190,294 per violation, per year** (Tier 4: Willful Neglect, Not Corrected).
Source: Federal Register 2026-01688, January 28, 2026.

Small practices usually settle in the middle tiers. A missing or inadequate Risk Analysis commonly settles for **$50,000 to $300,000**, often with a 2-to-3-year Corrective Action Plan and quarterly OCR check-ins. In the first four months of 2026, OCR collected more than $1.28 million in HIPAA settlements.

THE 20-MINUTE GUT CHECK

Ask one question: do we have a written Risk Analysis, signed and dated within the last 12 months, that covers every system touching ePHI?

If you are not sure, that uncertainty is the finding.

North Privacy Advisors does a flat $750 Privacy Exposure Review: 48 hours, your top three risks, no big commitment. It is the fastest way to know where you actually stand.

Reply to my email, or book a time at northprivacyadvisors.com.

Sam Cherkaoui, CIPP/US
sam@northprivacyadvisors.com