After a breach report: what HHS is likely to ask for

HHS's Office for Civil Rights (OCR) reviews breach reports that cover 500 or more people, and it can ask for documents in writing. Not every practice gets a letter. If you do, these are the documents it is likely to ask for. Reporting is common. About 20 small healthcare providers a month report a breach of 500 or more people to HHS (our count).

12 of 785

breach reviews OCR closed in 2024 ended in a settlement or penalty.

11 of 12

●●●●●●●●●●○

of those found the risk analysis missing or not up to the rule's standard (our count, HHS 2024 report to Congress).

ITEM & DESCRIPTION	REGULATION (45 CFR)
☐ **1. What happened and when.** A dated account, from discovery to fix. → Have it ready: your IT vendor's incident report.	164.308(a)(6)(ii)
☐ **2. Proof of notice, with dates.** To patients and HHS without unreasonable delay, and within 60 days of discovery. Media too, if more than 500 residents of one state were affected. → Have it ready: the patient letter, mailing record, HHS confirmation and any press release.	164.404, 164.406, 164.408
☐ **3. Your risk analysis.** A written review of what could expose electronic patient records. Expect to show the latest one and earlier ones. → Have it ready: your "Security Risk Analysis" report.	164.308(a)(1)(ii)(A)
☐ **4. Your risk management plan.** The fixes you made, with dates, including those since the breach. → Have it ready: your remediation or action list.	164.308(a)(1)(ii)(B)
☐ **5. Incident and breach policies.** Your written steps for handling incidents and notifying people. → Have it ready: your HIPAA policy manual.	164.308(a)(6)(i); 164.414(a)
☐ **6. Vendor contracts.** Business associate agreements (HIPAA contracts with vendors that handle patient data) for each vendor involved. → Have it ready: the signed agreements.	164.308(b)(3)
☐ **7. Training and discipline records.** Who was trained and when, and any discipline applied. → Have it ready: your training log and HR notes.	164.308(a)(5)(i); 164.308(a)(1)(ii)(C)
☐ **8. Access controls.** Who could open the affected systems, and how access is given and removed. → Have it ready: a user list with roles.	164.312(a)(1)
☐ **9. Activity reviews.** Proof that someone regularly checks the records of who opened what. → Have it ready: audit log reports and review notes.	164.308(a)(1)(ii)(D)
☐ **10. Encryption.** Whether the affected devices were encrypted (scrambled so outsiders cannot read them). If not, your written reason. → Have it ready: your IT vendor's encryption report.	164.312(a)(2)(iv)

IF YOU ONLY DO ONE THING

Find your risk analysis. Check its date, and check that it covers every system that holds patient records. In two recent cases that began with a breach report, it was the only finding: Comprehensive Neurology (April 2025) and Top of the World Ranch Treatment Center (February 2026).