HIPAA Security Risk Analysis Worksheet

One row for each place electronic protected health information (ePHI) lives in your practice. Write what could go wrong there, what already protects it, how likely and how bad a problem would be, and the fix you will make with a date.

What the Security Rule asks for

45 CFR 164.308(a)(1)(ii)(A), Risk analysis (Required):

> *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."*

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308

Where ePHI lives	Vendor or product	BAA on file (Y/N, date)	Threats and weak spots	Current safeguards	Likelihood (L/M/H)	Impact (L/M/H)	Risk level	Fix and target date
EHR / practice management								
Email								
Phone and texts								
Video platform								
Laptop and other devices								
Backups								
Paper records and scans								
Other:								

Likelihood and impact: L, M, or H. One simple way to set the risk level is to take the higher of the two; anything rated H gets a fix and a date.

Keep it, and keep it current

Keep this worksheet 6 years from the date you create it or the date it was last in effect, whichever is later (45 CFR 164.316(b)(2)(i)). The same section asks you to review documentation periodically and update it when your setup changes (164.316(b)(2)(iii)).

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316

On January 6, 2025, HHS published proposed changes to the Security Rule in the Federal Register (90 FR 898). It is a proposed rule. As of September 2026 no final rule has been published, so the current text quoted above is the one that applies.

https://www.govinfo.gov/app/details/FR-2025-01-06/2024-30983

Completed by: _____

Date completed: _____

Next review date: _____