Small-practice security risk review

A practical California working record - editable in Word

USE IT THIS WAY	DO NOT MISTAKE IT FOR THIS
Use for a periodic risk-analysis cycle and after a material system, vendor, location, or workforce change.	This is not a complete HIPAA risk analysis, penetration test, or certification of security.

Working record

Prepared by	
Reference (no names)	
Date opened	
Next review date	

Six review points

1	**[ ] Inventory electronic information** Map devices, applications, accounts, networks, backups, removable media, and vendor systems. **Your record:** _____ **Source:** HHS: Security Rule guidance
2	**[ ] Identify foreseeable threats** Consider loss, theft, misdelivery, credential compromise, malware, outage, insider access, and physical exposure. **Your record:** _____ **Source:** HHS: Security Rule guidance
3	**[ ] Record current safeguards** Document administrative, physical, and technical controls actually in use rather than planned. **Your record:** _____ **Source:** HHS: Security Rule guidance
4	**[ ] Assess gaps consistently** Use one documented method for likelihood, impact, and priority across systems. **Your record:** _____ **Source:** HHS: Security Rule guidance
5	**[ ] Assign corrective work** Give every accepted or remediated risk an owner, action, due date, and status. **Your record:** _____ **Source:** HHS: Security Rule guidance

6	**[ ] Preserve the analysis** Keep the evidence, decisions, and follow-up so the review is reproducible later. **Your record:** _____ **Source:** HHS: Security Rule guidance

Close the loop

Decision / next action	
Owner	
Due date	

Controlling sources

- HHS: Security Rule guidance

Educational information only. Not legal, clinical, tax, billing, or regulatory advice. Recheck every source before relying on an older saved copy. Do not put client-identifying information in a copy you cannot secure.