HIPAA AUDITORS

Evaluation Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.308(a)(8) — Evaluation

Issued	9 August 2026
Prepared by	HIPAA Auditors — certified HIPAA lead auditors
Contact	info@hipaaauditors.com · +91-95851-60363
Address	100 Congress Ave, Suite 2000, Austin, TX 78701

How to use this document. This is a working template, not a finished compliance artefact. Replace every bracketed placeholder with your organisation's own detail, delete the guidance notes, and have the result reviewed and formally adopted by your Privacy or Security Officer before you rely on it.

Regulatory basis. References are to the HIPAA Administrative Simplification regulations at 45 CFR Parts 160, 162 and 164, and to NIST SP 800-66 Rev. 2, *Implementing the HIPAA Security Rule*.

The requirement

Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI.

45 CFR 164.308(a)(8) · Administrative Safeguards

Risk level	Difficulty	Typical cost	Timeframe
High	Moderate	Medium	2-4 months

Implementation steps

- [ ] **Develop and implement comprehensive evaluation procedures including:**
- [ ] **Regular security assessments and evaluations**
- [ ] **Technical evaluation of security controls**
- [ ] **Non-technical evaluation of policies and procedures**
- [ ] **Environmental change impact assessments**
- [ ] **Operational change impact assessments**
- [ ] **Evaluation documentation and reporting**
- [ ] **Remediation planning and tracking**
- [ ] **Key components:**
- [ ] **- Periodic security evaluations**
- [ ] **- Technical control assessments**
- [ ] **- Policy and procedure reviews**
- [ ] **- Change impact assessments**
- [ ] **- Documentation of evaluation results**
- [ ] **- Remediation planning and tracking**

Evidence to produce and retain

Tick only where the artefact exists and you can say where it lives.

- [ ] **Evaluation procedures and schedule**
  Location: _____ Owner: _____
- [ ] **Technical evaluation criteria and methods**
  Location: _____ Owner: _____

- [ ] **Non-technical evaluation criteria and methods**
  Location: _____ Owner: _____
- [ ] **Environmental change assessment procedures**
  Location: _____ Owner: _____
- [ ] **Operational change assessment procedures**
  Location: _____ Owner: _____
- [ ] **Evaluation documentation templates**
  Location: _____ Owner: _____
- [ ] **Remediation planning procedures**
  Location: _____ Owner: _____
- [ ] **Evaluation reporting procedures**
  Location: _____ Owner: _____

How this gets tested

These are the procedures an auditor is likely to run. Self-test first.

- [ ] **Review evaluation procedures and schedule**
  Result: _____ Tested by / date: _____
- [ ] **Verify technical evaluation methods**
  Result: _____ Tested by / date: _____
- [ ] **Test non-technical evaluation processes**
  Result: _____ Tested by / date: _____
- [ ] **Review change impact assessment procedures**
  Result: _____ Tested by / date: _____
- [ ] **Verify evaluation documentation**
  Result: _____ Tested by / date: _____
- [ ] **Test remediation planning procedures**
  Result: _____ Tested by / date: _____
- [ ] **Review evaluation reporting**
  Result: _____ Tested by / date: _____
- [ ] **Conduct evaluation exercises**
  Result: _____ Tested by / date: _____

Common failures to check yourself against

- Lack of regular security evaluations
- Inadequate technical control assessments
- Insufficient policy and procedure reviews

- Failure to assess impact of changes
- Inadequate documentation of evaluations
- Lack of remediation planning
- Insufficient evaluation reporting

Beyond the minimum

- Conduct regular security evaluations
- Use standardized evaluation criteria
- Document all evaluation results
- Assess impact of all changes
- Develop remediation plans
- Track remediation progress
- Regular reporting to management
- Continuous improvement of evaluation processes

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.1.7 NIST Cybersecurity Framework: DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5 NIST SP 800-53: CA-1, CA-2, CA-3, CA-4, CA-5, CA-6, CA-7, CA-8, CA-9

Sign-off

Completed by	Title	Date
Reviewed by	**Title**	**Next review due**