HIPAA AUDITORS

Security Incident Procedures Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.308(a)(6) — Security Incident Procedures

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

Implement policies and procedures to address security incidents.

45 CFR 164.308(a)(6) · Administrative Safeguards

Risk level	Difficulty	Typical cost	Timeframe
Critical	Complex	High	3-6 months

Implementation steps

- [ ] **Develop and implement comprehensive security incident procedures including:**
- [ ] **Incident detection and reporting procedures**
- [ ] **Incident response team roles and responsibilities**
- [ ] **Incident classification and prioritization**
- [ ] **Incident containment and mitigation procedures**
- [ ] **Incident investigation and analysis procedures**
- [ ] **Incident documentation and reporting requirements**
- [ ] **Post-incident review and improvement procedures**
- [ ] **Key components:**
- [ ] **- Incident response plan**
- [ ] **- Incident response team**
- [ ] **- Incident detection and reporting**
- [ ] **- Incident classification system**
- [ ] **- Incident containment procedures**
- [ ] **- Incident documentation requirements**

Evidence to produce and retain

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

- [ ] **Security incident response plan**
  Location: _____ Owner: _____
- [ ] **Incident response team roles and responsibilities**
  Location: _____ Owner: _____
- [ ] **Incident detection and reporting procedures**
  Location: _____ Owner: _____

- [ ] **Incident classification and prioritization procedures**
  Location: _____ Owner: _____
- [ ] **Incident containment and mitigation procedures**
  Location: _____ Owner: _____
- [ ] **Incident investigation and analysis procedures**
  Location: _____ Owner: _____
- [ ] **Incident documentation and reporting requirements**
  Location: _____ Owner: _____
- [ ] **Post-incident review procedures**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Review security incident response plan**
  Result: _____ Tested by / date: _____
- [ ] **Test incident detection and reporting procedures**
  Result: _____ Tested by / date: _____
- [ ] **Verify incident response team training**
  Result: _____ Tested by / date: _____
- [ ] **Test incident classification and prioritization**
  Result: _____ Tested by / date: _____
- [ ] **Review incident containment procedures**
  Result: _____ Tested by / date: _____
- [ ] **Verify incident documentation requirements**
  Result: _____ Tested by / date: _____
- [ ] **Test post-incident review procedures**
  Result: _____ Tested by / date: _____
- [ ] **Conduct incident response exercises**
  Result: _____ Tested by / date: _____

Common failures to check yourself against

- Lack of security incident response plan
- Inadequate incident detection and reporting procedures
- Insufficient incident response team training
- Poor incident classification and prioritization
- Inadequate incident containment procedures

- Insufficient incident documentation
- Lack of post-incident review and improvement

Beyond the minimum

- Develop comprehensive incident response plan
- Establish trained incident response team
- Implement effective incident detection and reporting
- Use clear incident classification system
- Develop effective containment procedures
- Document all incident activities
- Conduct regular post-incident reviews
- Regular testing and updating of procedures

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.1.5 NIST Cybersecurity Framework: RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1, RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2 NIST SP 800-53: IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, IR-9, IR-10

Sign-off

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