HIPAA AUDITORS

Contingency Plan Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.308(a)(7) — Contingency Plan

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

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

45 CFR 164.308(a)(7) · Administrative Safeguards

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

Implementation steps

- [ ] **Develop and implement comprehensive contingency planning including:**
- [ ] **Data backup plan with regular backups and testing**
- [ ] **Disaster recovery plan with recovery time objectives**
- [ ] **Emergency mode operation plan for critical functions**
- [ ] **Testing and revision procedures for all plans**
- [ ] **Applications and data criticality analysis**
- [ ] **Emergency access procedures**
- [ ] **Communication plans for emergencies**
- [ ] **Key components:**
- [ ] **- Data backup and recovery procedures**
- [ ] **- Disaster recovery planning**
- [ ] **- Emergency mode operations**
- [ ] **- Business continuity planning**
- [ ] **- Regular testing and updating of plans**
- [ ] **- Critical system identification**

Evidence to produce and retain

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

- [ ] **Contingency plan document**
  Location: _____ Owner: _____
- [ ] **Data backup plan and procedures**
  Location: _____ Owner: _____

- [ ] **Disaster recovery plan**
  Location: _____ Owner: _____
- [ ] **Emergency mode operation plan**
  Location: _____ Owner: _____
- [ ] **Testing and revision procedures**
  Location: _____ Owner: _____
- [ ] **Applications and data criticality analysis**
  Location: _____ Owner: _____
- [ ] **Emergency access procedures**
  Location: _____ Owner: _____
- [ ] **Communication plans**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Review contingency plan documentation**
  Result: _____ Tested by / date: _____
- [ ] **Test data backup and recovery procedures**
  Result: _____ Tested by / date: _____
- [ ] **Verify disaster recovery capabilities**
  Result: _____ Tested by / date: _____
- [ ] **Test emergency mode operations**
  Result: _____ Tested by / date: _____
- [ ] **Review testing and revision procedures**
  Result: _____ Tested by / date: _____
- [ ] **Verify critical system documentation**
  Result: _____ Tested by / date: _____
- [ ] **Test emergency communication procedures**
  Result: _____ Tested by / date: _____
- [ ] **Conduct tabletop exercises**
  Result: _____ Tested by / date: _____

Common failures to check yourself against

- Lack of comprehensive contingency plan
- Inadequate data backup procedures
- Insufficient disaster recovery planning

- No emergency mode operation plan
- Failure to test contingency plans regularly
- Inadequate documentation of critical systems
- Insufficient emergency communication procedures

Beyond the minimum

- Develop comprehensive contingency planning
- Implement regular data backup procedures
- Create detailed disaster recovery plans
- Establish emergency mode operations
- Regular testing and updating of plans
- Document all critical systems and applications
- Establish clear communication procedures
- Coordinate with external service providers

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.1.6 NIST Cybersecurity Framework: RS.RP-1, RS.RP-2, RS.RP-3, RS.IM-1, RS.IM-2 NIST SP 800-53: CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-12, CP-13

Sign-off

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