HIPAA AUDITORS

Integrity Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.312(c)(1) — Integrity

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 protect ePHI from improper alteration or destruction.

45 CFR 164.312(c)(1) · Technical Safeguards

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

Implementation steps

	Implement policies and procedures to protect ePHI from improper alteration or destruction. The standard at 164.312(c)(1) is supported by one addressable specification, the mechanism to authenticate ePHI at 164.312(c)(2), which asks for electronic means to corroborate that data has not been altered or destroyed without authorisation
	Integrity failures are less visible than confidentiality failures and often more dangerous clinically: a silently altered allergy record or medication dose can cause direct patient harm, and ransomware that encrypts or corrupts records is an integrity and availability event as much as a confidentiality one
	Implementation approach:
	Restrict who can modify ePHI, and separate the ability to change data from the ability to change the audit trail
	Enforce validation at entry — type, range, format and clinical plausibility checks — so bad data is rejected rather than stored
	Maintain record versioning or an amendment history so prior values remain recoverable and visible
	Apply cryptographic corroboration where it is reasonable and appropriate: hashes or checksums on stored records, archives and exports, and digital signatures where authorship matters
	Verify integrity on transfer, backup and restore, and compare hashes rather than assuming success
	Protect against malware and ransomware, which are the most common cause of large-scale integrity loss
	Test restores regularly; an untested backup is an assumption, not a control
	Log and alert on unexpected bulk modification or deletion
	Where you decide not to implement the addressable authentication mechanism, document the reasoning and the alternative safeguard under 164.306(d)

Evidence to produce and retain

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

- [ ] **Data integrity policy and supporting procedures**
  Location: _____ Owner: _____
- [ ] **Data validation rules and where they are enforced**
  Location: _____ Owner: _____
- [ ] **Record versioning or amendment history design, and retention of prior values**
  Location: _____ Owner: _____
- [ ] **Integrity mechanism decision record for 164.312(c)(2), including equivalent alternatives where not implemented**
  Location: _____ Owner: _____
- [ ] **Checksum, hash or digital signature standard and the systems it covers**
  Location: _____ Owner: _____
- [ ] **Backup and restore procedures, with completed restore test records**
  Location: _____ Owner: _____
- [ ] **Malware and ransomware protection configuration and coverage evidence**
  Location: _____ Owner: _____
- [ ] **Change control records for systems processing ePHI**
  Location: _____ Owner: _____
- [ ] **Integrity incident records, including detection, investigation and correction**
  Location: _____ Owner: _____
- [ ] **Alert definitions for unexpected bulk modification or deletion**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Attempt to write invalid data and confirm validation rejects it rather than storing it**
  Result: _____ Tested by / date: _____
- [ ] **Modify a test record and confirm the prior value remains recoverable through version or amendment history**
  Result: _____ Tested by / date: _____
- [ ] **Verify hash or checksum generation and validation on stored records, archives and exports**
  Result: _____ Tested by / date: _____
- [ ] **Perform a full restore from backup into an isolated environment and compare against expected content**
  Result: _____ Tested by / date: _____
- [ ]

	Confirm integrity verification occurs on transfer and after restore, with recorded results Result: _____ Tested by / date: _____
	Attempt an unauthorised modification and confirm it is prevented, logged and alerted Result: _____ Tested by / date: _____
	Confirm malware protection is deployed, current and covering every system holding ePHI Result: _____ Tested by / date: _____
	Review change control records for a sample of recent changes to ePHI systems Result: _____ Tested by / date: _____
	Test the alert path for bulk deletion or modification end to end Result: _____ Tested by / date: _____
	Confirm the ability to modify data is separated from the ability to modify audit records Result: _____ Tested by / date: _____

Common failures to check yourself against

- No mechanism at all to detect that ePHI has been altered
- Backups configured but never restore-tested, so integrity is assumed rather than known
- All backup copies reachable from the production network, leaving nothing safe from ransomware
- Records overwritten in place with no version history, making improper alteration undetectable
- Weak or absent input validation allowing implausible clinical values to be stored
- Privileged users able to change both the data and the audit trail that would reveal it
- The addressable authentication mechanism dismissed with no documented decision
- Malware protection missing from servers, medical devices or cloud workloads
- Integrity treated purely as a backup question, with no detection component

Beyond the minimum

- Keep immutable or append-only audit trails so alteration of the record is always detectable
- Retain version history for clinical data rather than overwriting in place
- Hash records and archives at rest, and verify on access, transfer and restore
- Use digital signatures where authorship or non-repudiation matters, such as orders and consent
- Hold at least one backup copy offline or immutable so ransomware cannot reach it
- Test restores on a schedule and record the outcome, including time taken
- Alert on anomalous bulk change or deletion patterns rather than relying on discovery
- Apply strict change control to systems processing ePHI, including database schema changes
- Validate data at the point of entry, where correction is cheapest and safest

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.3.3

Sign-off

Completed by	Title	Date

Reviewed by	**Title**	**Next review due**

Want this verified independently? We test controls like this one on every HIPAA engagement. Request a scoped quote at https://hipaaauditors.com/contact