HIPAA AUDITORS

Transmission Security Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.312(e) — Transmission Security

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 technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

45 CFR 164.312(e) · Technical Safeguards

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

Implementation steps

	Implement technical security measures to guard against unauthorised access to ePHI transmitted over an electronic communications network. The standard at 164.312(e)(1) carries two addressable specifications: integrity controls at 164.312(e)(2)(i), and encryption at 164.312(e)(2)(ii)
	Start by inventorying every transmission path. Organisations consistently under-count these, and an uninventoried path cannot be protected. Typical paths include clinical interfaces and HL7 or FHIR feeds, email, SFTP and file transfer to payers and labs, remote access sessions, API integrations, cloud replication and backup, fax over IP, mobile applications, and messaging between clinicians
	Implementation approach:
	Encrypt ePHI in transit as the default. Use TLS 1.2 as a floor and prefer TLS 1.3, with strong cipher suites, certificate validation and no fallback to deprecated protocols
	Disable SSL 3.0, TLS 1.0 and TLS 1.1, and remove export-grade and NULL cipher suites
	Validate certificates properly, including chain and hostname; accepting invalid certificates silently negates the protection
	Apply integrity controls so undetected modification in transit is prevented — authenticated encryption modes achieve confidentiality and integrity together
	Secure email carrying ePHI through TLS with enforced policy, a portal, or message-level encryption. Opportunistic TLS alone is not enforcement
	Replace legacy plaintext protocols: FTP, Telnet, HTTP and unauthenticated SMTP relay
	Encrypt internal transmission too where risk warrants; a flat internal network is not a trust boundary
	Where you decide against encryption on a given path, record the reasoning and the equivalent alternative under 164.306(d). Encryption meeting HHS guidance is also the route to the safe harbour at 164.402
	Test what you configured. Scanning your own endpoints is the fastest way to find the path still negotiating TLS 1.0

Evidence to produce and retain

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

- [ ] **Transmission security policy and supporting procedures**
  Location: _____ Owner: _____
- [ ] **Inventory of every ePHI transmission path, with counterparty, protocol and encryption status**
  Location: _____ Owner: _____
- [ ] **Approved protocol and cipher suite standard, including minimum TLS version**
  Location: _____ Owner: _____
- [ ] **Encryption decision record per path, with equivalent alternatives where encryption is not used**
  Location: _____ Owner: _____
- [ ] **Integrity control design for transmission, covering 164.312(e)(2)(i)**
  Location: _____ Owner: _____
- [ ] **Email security configuration, including TLS enforcement or portal arrangements**
  Location: _____ Owner: _____
- [ ] **Certificate inventory, ownership and renewal schedule**
  Location: _____ Owner: _____
- [ ] **Scan or test results demonstrating configuration matches policy**
  Location: _____ Owner: _____
- [ ] **Business associate agreements covering each external transmission counterparty**
  Location: _____ Owner: _____
- [ ] **Records of transmission-related incidents**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Enumerate transmission paths independently and compare against the inventory to find omissions**
  Result: _____ Tested by / date: _____
- [ ] **Scan external endpoints and confirm the negotiated TLS version and cipher suites match policy**
  Result: _____ Tested by / date: _____
- [ ] **Attempt to connect using TLS 1.0 or a weak cipher and confirm the connection is refused**
  Result: _____ Tested by / date: _____
- [ ] **Present an invalid or expired certificate and confirm the client rejects it**
  Result: _____ Tested by / date: _____

	Capture traffic on a sample internal path and confirm ePHI is not observable in plaintext Result: _____ Tested by / date: _____
	Send a test message containing ePHI by email and verify encryption was actually applied, not merely attempted Result: _____ Tested by / date: _____
	Confirm legacy plaintext protocols are disabled by attempting to use them Result: _____ Tested by / date: _____
	Verify integrity protection by confirming authenticated encryption or an equivalent mechanism is in use Result: _____ Tested by / date: _____
	Check certificate expiry dates against the renewal schedule Result: _____ Tested by / date: _____
	Confirm a signed business associate agreement exists for every external counterparty receiving ePHI Result: _____ Tested by / date: _____

Common failures to check yourself against

- EPHI sent by unencrypted email, most often to patients or external clinicians
- Deprecated TLS versions or weak cipher suites still enabled on external endpoints
- Certificate validation disabled to make an integration work, silently removing the protection
- Legacy FTP or HTTP interfaces still carrying ePHI to partners
- Incomplete transmission inventory, so whole paths are never assessed
- The addressable encryption specification dismissed with no documented decision
- Internal traffic left unencrypted on the assumption that the internal network is trusted
- Expired certificates prompting insecure workarounds rather than renewal
- External transmission to a counterparty with no business associate agreement in place

Beyond the minimum

- Treat encryption in transit as the default and justify exceptions rather than the reverse
- Prefer TLS 1.3, with TLS 1.2 as the floor, and use authenticated encryption modes
- Enforce TLS for email to known partners rather than relying on opportunistic negotiation
- Monitor certificate expiry automatically; expiry causes both outage and insecure workaround
- Scan your own endpoints on a schedule and after every change, because configuration drifts
- Encrypt internal traffic where ePHI crosses network segments
- Retire legacy interfaces that cannot be secured rather than granting indefinite exceptions
- Keep the transmission inventory current as part of change control, not as an annual exercise
- Verify a BAA is in place before any new external transmission path goes live

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.3.5

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