FRAMEWORK MAPPING

HIPAA (45 CFR Parts 160, 162, 164)

Publisher. US HHS

Control mappings. 24 controls

Statement date. 2026-08-03

Health Insurance Portability and Accountability Act. Etch addresses the technical safeguards at 164.312, the administrative safeguards at 164.308, and the record retention posture at 164.316.

Control mapping

Every row names a specific control from the framework and describes how Etch addresses it. The response prose commits to what Etch signs on the chain, not to runtime enforcement. Etch is an evidence layer.

Control ref	Control name	How Etch addresses it
`164.308(a)(1)(ii)(A)`	Risk analysis	Session risk score field records the upstream vendor's risk assessment at each event. Risk analysis evidence is chain signed against the specific event.
`164.308(a)(1)(ii)(D)`	Information system activity review	The chain is the activity review substrate. Every recorded event is chain signed and externally anchored. Session scope verifier lets a reviewer walk a single patient related session without exposing the full project chain.
`164.308(a)(3)(ii)(B)`	Workforce clearance	Bounded authority receipt binds identity, scope, and expiration for each acting party. Workforce clearance is verifiable per event.
`164.308(a)(4)(ii)(A)`	Isolating health care clearinghouse	Token scope segregation (mcp:read, mcp:write, admin:project) enforces separation of duties. Cross chain federation lets a clearinghouse chain reference a health system chain without merging trust.

Control ref	Control name	How Etch addresses it
`164.308(a)(5)(ii)(C)`	Log in monitoring	Token issuance and revocation are chain signed via the admin API. Every session start is a chain signed model card attestation event.
`164.308(a)(6)(ii)`	Security incident procedures	Signed postmortem event records incident retrospective with about_event_id, finding, corrective_action, signer, and optional retroactive confidence downgrade.
`164.308(a)(7)(ii)(A)`	Data backup	Chain data replicates to a hot standby in a second availability zone. The hot cold storage split supports long term archival with Merkle path verification against cold data.
`164.308(a)(7)(ii)(D)`	Testing and revision	The offline verifier runs on chain state and reports on 11 check categories. Adversarial benchmark tests tamper detection continuously via public MIT reproducible harness.
`164.308(a)(8)`	Evaluation	Recoverability measurement, drift detection engine, corrigibility self audit all run on chain state. All measurements are chain signed.
`164.312(a)(1)`	Access control	Token scopes segregate access. Tokens hashed at rest. Bounded authority receipt verifies per event Ed25519 signatures against a per project pubkey registry.
`164.312(a)(2)(i)`	Unique user identification	Every event carries an identifiable signer via bounded authority receipt or signed dissent. Unique identity is chain signed at event level.
`164.312(a)(2)(ii)`	Emergency access procedure	Explicit stop condition events halt a session on chain. The verifier flags any post halt write in the same session scope.
`164.312(a)(2)(iii)`	Automatic logoff	Authority receipt expiration field bounds the effective window of each signer. Expired authority is detectable on chain.

Control ref	Control name	How Etch addresses it
`164.312(a)(2)(iv)`	Encryption and decryption	Signing keys are KMS encrypted under a KEK loaded at boot from hardware. HSM attestation endpoint lets a Covered Entity bring its own HSM (tpm2, yubikey, aws-nitro, gcp-shielded, azure-attestation, sev-snp, intel-tdx).
`164.312(b)`	Audit controls	The signed chain is the audit control substrate. SQL layer append only triggers reject UPDATE and DELETE. External anchoring to Sigstore Rekor and Bitcoin OpenTimestamps.
`164.312(c)(1)`	Integrity	SHA 256 Merkle chain per epoch. Hybrid Ed25519 and SLH-DSA-SHA2-128f envelope on every closed epoch. Post hoc modification breaks chain integrity and is detectable by the offline verifier.
`164.312(c)(2)`	Mechanism to authenticate ePHI	Every event on the chain is authenticated by the epoch signature envelope over the row's Merkle path. Individual event authentication is walkable offline.
`164.312(d)`	Person or entity authentication	Bounded authority receipt binds a chain event to a specific person or entity via Ed25519 signature verified against the per project pubkey registry.
`164.312(e)(1)`	Transmission security	All external traffic on TLS 1.2 or higher. Internal service traffic on 127.0.0.1 loopback only.
`164.312(e)(2)(i)`	Integrity controls in transmission	Chain evidence is transmitted with its signature envelope attached. Integrity verification is possible at any transmission boundary via the offline verifier.
`164.312(e)(2)(ii)`	Encryption in transmission	TLS 1.2 or higher with strict SNI. HSM attested signing keys never leave the HSM boundary in enterprise BYOK deployments.
`164.316(a)`	Policies and procedures	Every policy version is committed to the chain by policy_hash. Policy drift detector alerts when a downstream node is running a stale policy_hash.

Control ref	Control name	How Etch addresses it
`164.316(b)(1)`	Documentation	Artifact hash endpoint chain signs any documentation artifact by SHA 256. Documentation cannot be silently revised without a new chain signed event.
`164.316(b)(2)(i)`	Six year retention	Hot cold storage split supports long term archival with Merkle path verification against cold data. Retention posture is operator configurable.