NEXACC

Encryption and transmission security policy

NEXACC LLC - HIPAA compliance package v2026.1 - issued 2026-08-31
4750 S 44th Pl Suite 120, Phoenix, AZ 85040 - info@nexacc.com - +1 (443) 739-9197 - www.nexacc.com

How PHI and client financial records are protected in transit, at rest, in backups, and on endpoints.

Scope

This policy applies to all systems that store, process, or transmit protected health information or client financial records, and to every workforce member and subcontractor with access to those systems.

Encryption in transit

All web, portal, and API traffic is served exclusively over TLS 1.2 or higher with modern cipher suites; plaintext HTTP requests are 301-redirected to HTTPS and HSTS is enforced with max-age 31536000 and includeSubDomains.

Database and storage connections use TLS. Client document uploads travel from the browser directly to encrypted storage over TLS through an authenticated server function.

PHI is never sent as an email attachment. Internal notifications carry only a non-PHI reference and a short-lived signed link that resolves inside the vault.

Encryption at rest

Stored documents and database records are encrypted at rest with AES-256. Encryption keys are managed by the hosting platform's key management service and are not accessible to workforce members.

Backups are encrypted with the same standard and are subject to the same retention and access controls as production data.

Access to encrypted data

Row-level security policies scope every stored record to the owning client account; a signed-in client can read only their own data and staff access is role-based and individually provisioned.

Signed document links are time-limited and expire automatically; they are issued only to authorized recipients and each issuance is logged.

Multi-factor authentication is required for administrative access. Credentials are never shared between workforce members.

Endpoints and media

Workstations used for engagement work run full-disk encryption, automatic screen lock, current operating system patches, and endpoint protection.

Removable media is not used for PHI. Media and hardware that has held PHI is sanitized or destroyed in line with NIST SP 800-88 before disposal.

Verification and review

TLS configuration, security response headers, and dependency vulnerabilities are checked by an external scan on a scheduled basis and after every significant release.

This policy is reviewed at least annually and after any material change in systems or a reportable security incident.

Questions about this document: info@nexacc.com. NEXACC is not a covered entity; it acts as a business associate to the practices it serves.