# NEXACC

## HIPAA compliance package

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

The BAA template, encryption policy, and audit logging policy in a single document.

## BUSINESS ASSOCIATE AGREEMENT (TEMPLATE)

The agreement we execute with every covered entity before any protected health information moves, aligned to 45 CFR 164.504(e).

### 1. Parties and purpose

This Business Associate Agreement supplements the services agreement between the Covered Entity and NEXACC (Business Associate) and governs any Protected Health Information (PHI) created, received, maintained, or transmitted by NEXACC on the Covered Entity's behalf in the course of medical billing, revenue cycle management, credentialing, and related accounting services.

Terms used but not defined here have the meaning given in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164.

### 2. Permitted uses and disclosures

NEXACC may use or disclose PHI only to perform the services described in the underlying agreement, for its own proper management and administration, or as required by law.

NEXACC applies the minimum-necessary standard to every use, disclosure, and request for PHI.

NEXACC will not use or disclose PHI in a manner that would violate the Privacy Rule if done by the Covered Entity.

### 3. Safeguards

NEXACC implements the administrative, physical, and technical safeguards required by 45 CFR 164.308, 164.310, and 164.312, including access control, unique user identification, encryption of PHI in transit and at rest, audit controls, integrity controls, and transmission security.

NEXACC maintains written policies and procedures and retains required documentation for six years from the later of the date of creation or the date last in effect.

### 4. Subcontractors

NEXACC will ensure that any subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to restrictions and conditions at least as restrictive as those that apply to NEXACC under this agreement.

## 5. Reporting and breach notification

NEXACC will report to the Covered Entity any use or disclosure of PHI not permitted by this agreement, any security incident of which it becomes aware, and any Breach of Unsecured PHI.

Notification of a Breach will be made without unreasonable delay and no later than 30 calendar days after discovery, and will include the identification of each individual whose PHI was involved, together with the information required by 45 CFR 164.410(c) to the extent known.

## 6. Individual rights

NEXACC will make PHI in a Designated Record Set available to the Covered Entity so it can respond to access requests under 45 CFR 164.524 and amendment requests under 164.526.

NEXACC will document disclosures of PHI and related information and make it available so the Covered Entity can respond to an accounting of disclosures request under 45 CFR 164.528.

NEXACC will make its internal practices, books, and records relating to PHI available to the Secretary of Health and Human Services for purposes of determining compliance.

## 7. Term and termination

This agreement is effective on the date of execution and terminates when all PHI is returned or destroyed, or protections are extended to any PHI that cannot feasibly be returned or destroyed.

The Covered Entity may terminate the underlying agreement if NEXACC materially breaches this agreement and does not cure the breach within 30 days of written notice.

## 8. Execution

Covered Entity: _____ Signature: _____ Date: _____

NEXACC: _____ Signature: _____ Date: _____

# ENCRYPTION AND TRANSMISSION SECURITY POLICY

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.

## AUDIT LOGGING AND DISCLOSURE ACCOUNTING POLICY

What we record, how long we keep it, and how a covered entity can request an accounting of disclosures.

### Purpose

This policy implements the audit controls standard at 45 CFR 164.312(b) and supports the accounting of disclosures right at 45 CFR 164.528.

## Events recorded

Authentication events: sign-in, sign-out, failed attempts, and password or access changes.

Document events: upload, metadata change, signed-link issuance, and download, each with actor, timestamp, client account, and file reference.

Administrative events: role grants and revocations, client account and membership changes, template and integration changes.

Outbound communications: every email attempt with channel, recipient, subject, delivery status, provider message identifier, and any failure detail.

Data changes: inserts, updates, and status transitions on client records, with the acting identity retained.

## Integrity of the log

Audit records are append-only to application roles: the application cannot update or delete entries, and log tables carry policies that deny modification and deletion.

Records are written server-side from the trusted execution path, not from the browser, so a client cannot suppress or forge an entry.

## Retention and review

Audit records are retained for at least six years, consistent with the HIPAA documentation retention requirement.

Logs are reviewed on a recurring basis, and immediately following any suspected security incident or unusual access pattern. Findings are documented with the remediation taken.

## Accounting of disclosures

A covered entity may request an accounting of disclosures of its PHI by writing to info@nexacc.com. We respond within 30 days with the date, recipient, description, and purpose of each accountable disclosure within the requested period, up to six years.

Because disclosure activity is derived from retained audit records rather than recollection, the accounting can be produced as an exported record.

## Incident and breach handling

Suspected incidents are triaged the same business day, contained, and documented in an incident register with scope, root cause, and remediation.

Where a Breach of Unsecured PHI is confirmed, the covered entity is notified without unreasonable delay and no later than 30 calendar days after discovery, with the information required by 45 CFR 164.410(c).

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

to the practices it serves.