NEXACC

Security & data-handling brief

Guide - Written for the partner who has to sign off on a vendor: access control, workspace separation, credential handling, logging, PHI, confidentiality and exit cleanup.

For accounting, tax, bookkeeping, payroll and medical billing firms

Written for the partner or IT reviewer who has to sign off on a vendor. Send us your own questionnaire, insurance requirements and data-processing terms during the paper stage and we complete them before any file moves.

Controls at a glance

Access model: Least-privilege, granted per file, approved by the engagement lead

Separation: One workspace and credential store per partner firm; no pooled data

Credentials: Named users in your tenant where supported; vault-stored, rotated on roll-off

Logging: Access grants, removals and file activity logged; history available on request

PHI: BAA signed before any protected health information moves; minimum-necessary access

Confidentiality: Mutual NDA, non-solicitation and non-circumvention for the term plus 24 months

Exit: Complete portable file, access revoked in one business day, working copies deleted in 30 days

Detail

Who at NEXACC can see our client data?

Only the named preparer and reviewer assigned to that file, plus the engagement lead. Access is least-privilege and granted per file rather than per firm, so an accountant on one of your clients cannot open another. New access requires the engagement lead's approval and is recorded.

How is our firm's data separated from other partners' data?

Each partner firm gets its own workspace and its own credential store. Files, documents and credentials are never pooled across partner firms, and our internal tooling scopes every record to a single workspace so a cross-firm query is not possible in the first place.

How do you handle credentials for our systems?

Wherever the platform supports it we use a named user inside your tenant with the minimum role required, so you can see and revoke us directly. Shared credentials are a last resort, stored in an access-controlled vault, never emailed or kept in spreadsheets, and rotated when a team member rolls off.

What is logged, and can we see it?

Access grants, access removals and file-level activity are logged. Partner firms can request the access history for their workspace at any time, and it is included as standard in offboarding documentation.

How do you protect protected health information?

A BAA is signed before any PHI moves. PHI stays in the client's or your own systems wherever possible, minimum-necessary access applies to every request, and billing staff working PHI are assigned per practice rather than pooled.

What are your confidentiality terms?

Mutual NDA plus mutual non-solicitation and non-circumvention covering your clients and staff for the term plus 24 months, signed before we see a ledger. Every NEXACC team member is under an individual confidentiality agreement that survives their employment.

Do you use our data to train AI tools or for marketing?

No. Partner and client data is never loaded into marketing systems, never used to build lookalike audiences, and never submitted to third-party model training. Where we use software with AI features, it runs under business terms that exclude training on our tenant's content.

What happens to our data when the engagement ends?

You get the complete working file first - current, tied out, in a portable format, with no exit fee. Our access to your systems is revoked within one business day of the end date. Working copies held on our side are deleted within 30 days, except records we are required to retain, which stay under the same confidentiality terms. You receive written confirmation when cleanup is done.

What happens if a NEXACC team member leaves mid-engagement?

Their access is revoked the same day, the documented backup for that seat picks up the file, and you are told who changed. Confidentiality obligations survive their departure.

Will you complete our security questionnaire or vendor review?

Yes. Send us your questionnaire, insurance requirements and data-processing terms during the paper stage and we complete them before any file moves - that step is built into the onboarding sequence, not bolted on afterwards.

Offboarding timeline

Day 0 - End date confirmed in writing; final working file prepared and tied out.

Day 1 - All NEXACC access to your systems revoked; access history exported to you.

Day 1-5 - Complete workpapers delivered in a portable format, no exit fee.

Day 30 - Working copies on our side deleted; written cleanup confirmation issued.

Talk it through

A 30-minute fit call, no deck: what is backing up, which client profiles you would hand over, and what a pilot on two or three files would cost.

Book a fit call: https://www.nexacc.com/schedule

info@nexacc.com - +1 (443) 739-9197 - www.nexacc.com/partners