COUNTSURE

NDA & CONFIDENTIALITY CHECKLIST FOR CPA FIRMS USING OFFSHORE SERVICES

COUNTSURE.COM

NDA & Confidentiality Checklist for CPA Firms Using Offshore Services 10 Contract Provisions to Verify Before Sharing Any Client Data For CPA Firm Partners & Accounting Firm Managers

2026 Edition

WHY THIS CHECKLIST EXISTS

When a CPA firm shares client financial data with an offshore accounting provider, the legal obligation to protect that data does not transfer — it stays with your firm. A strong Non-Disclosure Agreement is not a formality. It is the primary contractual mechanism that defines what your offshore partner is obligated to protect, how they must respond if something goes wrong, and what remedies your firm has if they fail.

Most NDAs used by offshore providers are generic, self-serving documents that protect the provider - not your firm or your clients. This checklist identifies the 10 provisions that every CPA firm should verify are present in any NDA before sharing a single client file.

□ **CRITICAL** — Must Be Present
□ **IMPORTANT** — Verify Before Signing
□ **STANDARD** — Best Practice

SECTION - A

Scope & Coverage

01 | □ | The NDA Covers All Staff with Access — Not Just the Organization □ CRITICAL

Does the NDA explicitly bind individual employees, contractors, and subcontractors who will access your client data - not just the offshore firm as a corporate entity? A company-level NDA that does not extend to individual staff members creates a gap that is difficult to enforce in the event of a leak by a junior team member. Request confirmation that all staff sign individual confidentiality agreements as a condition of employment.

02 | ☐ | Confidential Information Is Defined Specifically - Not Generically ☐ CRITICAL

Does the NDA define "Confidential Information" in terms that explicitly include client financial records, tax return data, payroll information, entity structures, and any personally identifiable information (PII) your firm shares? Generic definitions such as "any business information" are vague and difficult to enforce. The definition should be specific enough that there is no ambiguity about what is protected.

03 | ☐ | The NDA Restricts Use to the Agreed Purpose Only ☐ CRITICAL

Does the NDA explicitly state that client data may only be used to perform the services outlined in the service agreement - and prohibit any secondary use, analysis, aggregation, or disclosure for any other purpose? Offshore providers should never be permitted to use your client data for training internal systems, benchmarking, or any purpose beyond direct service delivery.

SECTION - B

Data Handling Obligations

04 | □ | Restrictions on Copying, Downloading, and Storage Are Explicit □ CRITICAL

Does the NDA specify that client data may not be downloaded to personal devices, stored on unencrypted media, printed without authorization, or retained beyond the engagement period? Vague language about "taking reasonable precautions" is insufficient. The restrictions should mirror your firm's own data handling policies and should be specific enough to be enforceable.

05 | □ | Data Return and Destruction Obligations Are Defined □ IMPORTANT

Does the NDA specify what happens to your client data when the engagement ends — including a timeline for data return or certified destruction and a confirmation process? The provider should not be permitted to retain client data indefinitely after the relationship ends. Confirm the mechanism for data return and whether you receive written certification of destruction.

06 | □ | Subcontractor and Third-Party Disclosure Is Controlled □ IMPORTANT

Does the NDA require the offshore provider to obtain your written consent before sharing client data with any subcontra -ctor, technology platform, or third-party tool - and does it make the provider responsible for any third-party breach? Cloud tools, AI platforms, and freelance reviewers used without disclosure are common hidden risks in offshore workflows.

SECTION - C

Breach Response & Enforcement

07 | □ | Breach Notification Timeline Is Specified — Not Just "Promptly" □ CRITICAL

Does the NDA define a specific, maximum timeframe within which the provider must notify your firm of any actual or suspected data breach — ideally 24 to 48 hours? Language such as "promptly" or "as soon as practicable" is unenforceable and leaves the definition of timely notification entirely to the provider's discretion. Insist on a numeric deadline.

08 | □ | Remedies and Liability Are Defined — Not Capped at Zero □ CRITICAL

Does the NDA specify the remedies available to your firm in the event of a breach — including the right to seek injunctive relief and financial damages? Many offshore NDAs contain liability caps that limit the provider's exposure to the value of fees paid, leaving your firm exposed to far greater client-facing costs. Review the liability clause carefully with legal counsel before signing.

SECTION - D

Regulatory Alignment & Term

09 | □ | The NDA References Applicable US Regulatory Obligations □ IMPORTANT

Does the NDA acknowledge that your firm operates under IRS Circular 230, AICPA ethics rules, and applicable state CPA licensing requirements — and that the provider's confidentiality obligations are designed to support, not conflict with, your firm's compliance duties? A provider that is unaware of AICPA ET Section 1.700.040 cannot credibly claim to understand its obligations to a CPA firm.

10 | □ | The Confidentiality Obligation Survives Termination of the Agreement □ STANDARD

Does the NDA specify that confidentiality obligations remain in force after the service agreement ends — and for how long? A confidentiality obligation that expires when the contract ends provides no protection for data shared during the engagement. Best practice is a post-termination obligation of at least three to five years, or indefinitely for personally identifiable information.

HOW TO USE YOUR RESULTS

10 / 10

NDA Is Fit for Purpose. All critical protections are present. Proceed to signature after having legal counsel review the specific language.

7 – 9 / 10

Request Amendments Before Signing. Identify all missing provisions and return the NDA to the provider for revision. Do not proceed on a verbal assurance that missing terms will be "covered in the SOW."

6 or below / Any CRITICAL Item Missing

Do Not Sign. An NDA with fundamental gaps in coverage, breach notification, or liability does not protect your firm or your clients. Engage a different provider or require a complete redraft before proceeding.

See Countsure's NDA and Confidentiality Framework

Countsure provides every CPA firm partner with a comprehensive NDA before work begins — covering all staff, restricting data use to agreed services only, and specifying a 24-hour breach notification obligation. We welcome scrutiny. Bring this checklist to your call with us.

Review Our Terms — Schedule a Free 15-Minute Call

countsure.com

NDA & CONFIDENTIALITY CHECKLIST FOR CPA FIRMS USING OFFSHORE SERVICES

COUNTSURE.COM

NDA & Confidentiality Checklist for CPA Firms Using Offshore Services 10 Contract Provisions to Verify Before Sharing Any Client Data For CPA Firm Partners & Accounting Firm Managers

2026 Edition

WHY THIS CHECKLIST EXISTS

When a CPA firm shares client financial data with an offshore accounting provider, the legal obligation to protect that data does not transfer — it stays with your firm. A strong Non-Disclosure Agreement is not a formality. It is the primary contractual mechanism that defines what your offshore partner is obligated to protect, how they must respond if something goes wrong, and what remedies your firm has if they fail.

Most NDAs used by offshore providers are generic, self-serving documents that protect the provider - not your firm or your clients. This checklist identifies the 10 provisions that every CPA firm should verify are present in any NDA before sharing a single client file.

□ **CRITICAL** — Must Be Present

□ **IMPORTANT** — Verify Before Signing

□ **STANDARD** — Best Practice

SECTION - A

Scope & Coverage

01 | □ | The NDA Covers All Staff with Access — Not Just the Organization □ CRITICAL

Does the NDA explicitly bind individual employees, contractors, and subcontractors who will access your client data - not just the offshore firm as a corporate entity? A company-level NDA that does not extend to individual staff members creates a gap that is difficult to enforce in the event of a leak by a junior team member. Request confirmation that all staff sign individual confidentiality agreements as a condition of employment.

02 | □ | Confidential Information Is Defined Specifically - Not Generically □ CRITICAL

Does the NDA define "Confidential Information" in terms that explicitly include client financial records, tax return data, payroll information, entity structures, and any personally identifiable information (PII) your firm shares? Generic definitions such as "any business information" are vague and difficult to enforce. The definition should be specific enough that there is no ambiguity about what is protected.

03 | □ | The NDA Restricts Use to the Agreed Purpose Only □ CRITICAL

Does the NDA explicitly state that client data may only be used to perform the services outlined in the service agreement - and prohibit any secondary use, analysis, aggregation, or disclosure for any other purpose? Offshore providers should never be permitted to use your client data for training internal systems, benchmarking, or any purpose beyond direct service delivery.

SECTION - B

Data Handling Obligations

04 | □ | Restrictions on Copying, Downloading, and Storage Are Explicit □ CRITICAL

Does the NDA specify that client data may not be downloaded to personal devices, stored on unencrypted media, printed without authorization, or retained beyond the engagement period? Vague language about "taking reasonable precautions" is insufficient. The restrictions should mirror your firm's own data handling policies and should be specific enough to be enforceable.

05 | □ | Data Return and Destruction Obligations Are Defined □ IMPORTANT

Does the NDA specify what happens to your client data when the engagement ends — including a timeline for data return or certified destruction and a confirmation process? The provider should not be permitted to retain client data indefinitely after the relationship ends. Confirm the mechanism for data return and whether you receive written certification of destruction.

06 | □ | Subcontractor and Third-Party Disclosure Is Controlled □ IMPORTANT

Does the NDA require the offshore provider to obtain your written consent before sharing client data with any subcontra-ctor, technology platform, or third-party tool - and does it make the provider responsible for any third-party breach? Cloud tools, AI platforms, and freelance reviewers used without disclosure are common hidden risks in offshore workflows.

SECTION - C

Breach Response & Enforcement

07 | □ | Breach Notification Timeline Is Specified — Not Just "Promptly" □ CRITICAL

Does the NDA define a specific, maximum timeframe within which the provider must notify your firm of any actual or suspected data breach — ideally 24 to 48 hours? Language such as "promptly" or "as soon as practicable" is unenforceabl and leaves the definition of timely notification entirely to the provider's discretion. Insist on a numeric deadline.

08 | □ | Remedies and Liability Are Defined — Not Capped at Zero □ CRITICAL

Does the NDA specify the remedies available to your firm in the event of a breach — including the right to seek injunctive relief and financial damages? Many offshore NDAs contain liability caps that limit the provider's exposure to the value of fees paid, leaving your firm exposed to far greater client-facing costs. Review the liability clause carefully with legal counsel before signing.

SECTION - D

Regulatory Alignment & Term

09 | □ | The NDA References Applicable US Regulatory Obligations □ IMPORTANT

Does the NDA acknowledge that your firm operates under IRS Circular 230, AICPA ethics rules, and applicable state CPA licensing requirements — and that the provider's confidentiality obligations are designed to support, not conflict with, your firm's compliance duties? A provider that is unaware of AICPA ET Section 1.700.040 cannot credibly clain to understand its obligations to a CPA firm.

10 | □ | The Confidentiality Obligation Survives Termination of the Agreement □ STANDARD

Does the NDA specify that confidentiality obligations remain in force after the service agreement ends — and for how long? A confidentiality obligation that expires when the contract ends provides no protection for data shared during the engagement. Best practice is a post-termination obligation of at least three to five years, or indefinitely for personally identifiable information.

HOW TO USE YOUR RESULTS

10 / 10

NDA Is Fit for Purpose. All critical protections are present. Proceed to signature after having legal counsel review the specific language.

7 – 9 / 10

Request Amendments Before Signing. Identify all missing provisions and return the NDA to the provider for revision. Do not proceed on a verbal assurance that missing terms will be "covered in the SOW."

6 or below / Any CRITICAL Item Missing

Do Not Sign. An NDA with fundamental gaps in coverage, breach notification, or liability does not protect your firm or your clients. Engage a different provider or require a complete redraft before proceeding.

See Countsure's NDA and Confidentiality Framework

Countsure provides every CPA firm partner with a comprehensive NDA before work begins — covering all staff, restricting data use to agreed services only, and specifying a 24-hour breach notification obligation. We welcome scrutiny. Bring this checklist to your call with us.

Review Our Terms — Schedule a Free 15-Minute Call

countsure.com