Clean Source Data

CLIENT GUIDE 3 OF 4

Data Security and Transfer

How your data is processed inside your office, what leaves and how, and the safeguards we require from every buyer.

PREPARED BY
Clean Source Data

DOCUMENT
Data Security and Transfer

EDITION
November 2026

CLEAN SOURCE DATA | CLIENT GUIDE 3 OF 4

Data Security and Transfer

This overview covers on-site processing, delivery, access and cleanup. Permitted uses, retention and deletion are set in the license agreement you approve for each deal.

> **A NOTE ON AI BUYERS**
> Every AI company runs its own intake process, and tools, timelines and controls differ from buyer to buyer. This guide describes the standards Clean Source Data holds every buyer to. Before anything moves, your Clean Source project lead confirms the specific buyer's process and walks you through it.

01 Our Principles

CONTROL

Nothing moves without your approval

You choose what is included, who it goes to and when. A clean sample goes to a buyer only after you approve it in writing.

ON-SITE

Raw data never leaves your office

De-identification runs on a dedicated offline device at your location. Only the clean, approved package is ever delivered.

MINIMAL EXPOSURE

Descriptions before data

Valuation and buyer matching use descriptions, counts and schemas, not files. Your company can stay anonymous until you approve disclosure.

VERIFICATION

Every step is checked

Record counts and file manifests are reconciled at extraction and at delivery. Anything that does not match is investigated, never assumed complete.

02 How Your Data Moves

Unlike brokers that give a buyer's engineer access to your systems, our model keeps every raw record on your premises.

STAGE	WHAT HAPPENS
On-site setup	We bring a dedicated, offline processing device and an encrypted working drive to your location. No internet connection is used during processing.
Extraction	Your team runs or approves read-only exports of only the systems and date ranges in the agreed scope. No one needs ongoing access to your software.
De-identification	Identifiers are removed or replaced on the device, to the HIPAA Safe Harbor standard. Substitution keys stay on-site and are destroyed after delivery.
Your review	You spot-check a sample of the clean output and approve it in writing before anything is released.
Delivery	Only the approved, de-identified package is delivered: by encrypted transfer to storage dedicated to your deal, or by encrypted drive for very large packages.
Buyer verification	The buyer runs its own internal analysis to confirm the package is properly de-identified and no sensitive information remains, before accepting it.

TWO LAYERS OF PROTECTION

Many brokers send data to the AI company and let the buyer handle de-identification. We clean it inside your office first, you approve it, and then the buyer independently verifies it. Two separate teams have to agree it is clean before it is accepted.

03 Standards We Require From Every Buyer

SAFEGUARD	WHAT IT MEANS FOR YOU
Isolation	Your package lands in storage dedicated to your company and is not mixed with other companies' data.
Encryption	Data is encrypted in transit (TLS 1.2 or later) and at rest.

SAFEGUARD	WHAT IT MEANS FOR YOU
Access control	Access is time-limited, revocable and limited to named people responsible for the transfer.
Independent verification	The buyer must run its own privacy review of the delivered package and report anything that looks identifiable, rather than relying on our process alone.
No re-identification	The license prohibits the buyer from attempting to identify any person or business in the data.
Logging	Transfers and access grants and revocations are recorded.
Retention and deletion	How long the buyer keeps your data, and when it must delete it, is written into the license you approve.
Incident notice	The buyer must notify you promptly of any unauthorized access, within a deadline set in the license.

04 The Engagement Lifecycle

1. **Scope.**
   You and your project lead confirm the systems, date ranges, exclusions and delivery method.
   Our role: we document the scope and check it against your approved data inventory.

2. **Setup.**
   The offline device and encrypted drive are installed at your location.
   Our role: we confirm the device has no network connection before any data is loaded.

3. **Processing and review.**
   Data is extracted, de-identified and sampled for your approval.
   Our role: automated detection plus human review, with a written de-identification summary for your records.

4. **Delivery and verification.**
   The clean package is delivered, reconciled against the manifest, and independently checked by the buyer for any remaining sensitive information.
   Our role: we confirm counts match, and we resolve anything the buyer flags before acceptance.

5. **Cleanup.**
   Working drives are securely wiped and temporary access is revoked.
   Our role: we confirm cleanup in writing.

05 If Something Goes Wrong

Report any suspected problem (a transfer failure, unexpected access, a scope mismatch) to your project lead right away. We pause the process, escalate with the buyer's security, privacy or legal team, and track it until it is resolved.

Questions?

Your Clean Source project lead is your single point of contact.

info@cleansourcedata.com
cleansourcedata.com