DRAFT: placeholder pending counsel review. Not yet in effect.

Data Protection Agreement, with business associate terms

This Data Protection Agreement, referred to here as the DPA, governs Claracord's handling of the Records the Firm uploads. The Firm accepts it together with the Master Services Agreement, referred to here as the MSA, and it is part of that agreement.

One uniform DPA is offered to every client, whether or not HIPAA applies to that client. A plaintiff firm obtaining records by patient authorization and a payer subject to HIPAA receive identical protections, and no client has to work out which tier it is on.

1. Definitions

The terms business associate, covered entity, protected health information, required by law, subcontractor, unsecured protected health information, use and disclosure have the meanings given to them at 45 CFR 160.103. Those definitions are incorporated into this DPA by reference to that section and are not restated here.

Where the Firm is a covered entity or is itself a business associate, Claracord is the Firm's business associate for the Records the Firm uploads, and this DPA is the business associate agreement between them. Where the Firm is neither, the same terms apply as a matter of contract.

Claracord, the Firm, Records, Deliverables, the Services and the Portal have the meanings given to them in the MSA.

2. Permitted uses and disclosures

Claracord uses and discloses Records only to perform the Services, and for no other purpose.

Claracord does not sell Records or Deliverables and does not license them. Claracord discloses them to the Firm, to a destination the Firm directs Claracord to send them to, and to a subprocessor named in section 4 acting to perform the Services. To no one else.

No Record, and no part of one, is used to train, fine-tune or evaluate a model. Claracord does not sell, license or publish anything derived from a Record, and does not use a Record for marketing.

Claracord keeps two records of its own work that outlive the Records they came from, and this is the whole of what it keeps. The first is a skeleton of the human review: which question was asked, which page it was about, which answer the reviewer gave, which reviewer, and when. The second is a count, per case, of the kinds of correction a reviewer made, taken from a fixed list of correction types and held as whole numbers.

Of a Record, exactly one value is kept as it appears: the Bates label printed on the page, which is how a kept decision names the page it was about. A Bates label carries whatever prefix the Firm chose for its own production, so where that prefix names a provider or a custodian, that name is kept with it. Every other value a reviewer typed or read from a Record -- a patient name, a provider name, a date of service, a corrected value, any line of a document -- is kept only as a keyed one-way hash

of itself, under a key held outside the log, and cannot be read from it. No text of a Record is kept. What is kept beside the Bates label is timestamps, counts, the identifiers Claracord minted, and the fixed words of Claracord's own review questions and answers.

Claracord uses these two records to prove what its reviewers did and to find and fix repeated defects in its own process. They are shown to no other client and are not sold.

Claracord creates no other data set from Records and de-identifies them for no other purpose.

Claracord uses and discloses a Record where the law requires it, and tells the Firm before doing so where the law permits Claracord to tell it.

3. Safeguards

Claracord maintains the administrative, physical and technical safeguards stated in its Security Overview, published at portal.claracord.com/security. That page states what is built and marks what is not. This section promises nothing that the Portal does not do.

- Records are encrypted in transit and encrypted at rest.
- Each firm's Records are isolated from every other firm's, and every request for a Record is authorized against the firm the Record belongs to before the Record is read.
- Processing happens in the United States, as section 5 states.
- Operator access is reachable only through Cloudflare Access, and every request to it is checked for a signed assertion with a valid signature, audience, issuer and expiry. Multi-factor authentication is not yet enforced at the identity provider Cloudflare Access signs operators in with.
- Opening a case and downloading a Deliverable are each logged, with the Firm user, the case and the time. Claracord's own review of a Record is logged, with the reviewer, the page and the time. Reading one page of a Record inside a case already open is not logged as an entry of its own.

Claracord tells the Firm of a material change to these safeguards.

4. Subprocessors

Claracord uses these subprocessors and no others:

- Amazon Web Services, for hosting and storage.
- Stripe, for payments.
- Cloudflare, for network access and for TLS termination.
- Google Workspace, for email.

Claracord gives the Firm notice before it adds or changes a subprocessor. The Firm may object in writing within thirty days of that notice. On the Firm's objection the Firm may terminate the MSA, and is charged nothing for work not yet delivered.

Claracord holds a business associate agreement with Amazon Web Services, accepted on 16

September 2026, and with Google Workspace, executed on 22 September 2026. Stripe is sent an amount and Claracord's own identifiers for the case and the Firm, and no part of a Record. Claracord holds no business associate agreement with Cloudflare, which terminates TLS and is in the path of every byte.

Where the Firm connects its own Clio account, Claracord sends a Deliverable to the matter the Firm binds it to, in the United States and nowhere else. Clio is the Firm's own system and not a Claracord subprocessor: Claracord sends what the Firm directs and holds no account there of its own.

5. Personnel and location of processing

Records are stored and processed on servers in the United States. Human review is performed by Claracord's United States workforce.

Traffic to the Portal is encrypted in transit and passes through Cloudflare's network, which terminates TLS and may route that traffic through locations outside the United States. Cloudflare is named as a subprocessor in section 4.

Every person with access to a Record is bound by a written confidentiality obligation. Access is granted only to the people who need it to perform the Services.

The identity of the person who reviewed a case is recorded in Claracord's audit log, and is given to the Firm on request. It is not printed on a Deliverable.

6. Incident and breach notice

Claracord notifies the Firm of a security incident affecting the Firm's Records without unreasonable delay after discovering it, and in no case later than the sixty days 45 CFR 164.410 allows a business associate.

The notice states what happened, what data was involved, what Claracord has done and is doing about it, and whom at Claracord to contact. Claracord supplements the notice as it learns more, and does not hold the first notice back for a complete account.

Claracord cooperates with the Firm in any notification the Firm is required to make.

7. Return or destruction

On termination of the MSA, Claracord returns or destroys the Firm's Records and Deliverables. The Firm elects which. Absent an election, Claracord destroys them.

While the MSA is in force, Claracord retains a Record for the period stated in section 6 of the MSA, which is 90 days after delivery, or 14 days after the quote where the quote is not approved. Files are deleted after 90 days, sooner on request. A failed case is deleted 90 days after it was created. A quote expires after 14 days; an unaccepted quote and its upload are deleted then. A case is deleted sooner at the firm's request, and every deletion is logged.

Where the law requires a Record to be retained, Claracord retains that Record, only for as long as the law requires, and continues to apply this DPA to it. Claracord tells the Firm which Records were

retained and on what basis.

The audit log survives the return or destruction of the Records it describes. A log deleted with its records is not a record of access.

8. Audit and questionnaires

On request, Claracord provides its Security Overview, which is published at portal.claracord.com/security. Claracord publishes no pre-answered vendor questionnaire; where the Firm sends its own, Claracord answers it, including a question the Security Overview does not cover.

Claracord does not host an on-site audit, and grants no access to its systems or its network for the purpose of an audit.

9. Term

This DPA runs for the life of the MSA.

Sections 2, 5, 6 and 7 survive termination of the MSA for as long as Claracord holds any Record of the Firm. Section 7 survives until the return or destruction it requires is complete.

Version 1.10-draft

Document hash (SHA-256):
be616c39fe6d580868e94c3856d3d6ac741a1b9577dab613cc835c32b84aad02