

# Contracting for AI in Clinical Trials: Data Rights, Compliance, and Risk Allocation, Part Two

04-22-26 • alert • [katherine leibowitz](#)

This is the second installment of our two-part series on artificial intelligence (AI) in clinical trial operations.

**Part 1** describes where AI appears in clinical trial operations and the questions organizations should be asking. **Part 2** focuses on the contract provisions that address the resulting risks, particularly intellectual property, data rights, regulatory compliance, cybersecurity, monitoring and validation, and risk allocation. Each section lists key contract clauses to review. Even where not listed separately, indemnification and limitation of liability should be considered throughout.

Many agreements now include AI-specific provisions. There is no standard form, and their content varies depending on how AI is used and the risks involved. The issues below span multiple contract provisions and should be considered in that context.

For purposes of this post, “Data” refers broadly to data, documents, communications, and other information relating to the clinical trial, including outputs generated by AI systems using such information.

## I. Intellectual Property and Data Ownership

[Contract Clauses: Intellectual Property | Data License | Representations and Warranties | Audit](#)

Organizations should assess who owns:

- Data inputs
- AI-generated outputs
- Data used to train the AI
- The trained model or AI tool itself

It is also important to determine whether the contracting party owns the technology it uses or relies on third-party vendors that embed AI functionality.

Depending on the role of the AI and level of risk involved, it may be appropriate to obtain contractual assurances regarding ownership and licensing rights.

## II. Data Rights and Secondary Use

[Contract Clauses: Data License | Intellectual Property | AI | Confidentiality | EHR | HIPAA | Audit | Documentation | Termination Obligations | Storage and Retention | Indemnification](#)

One of the most consequential issues in AI contracting is how Data may be used after it enters an AI system, particularly whether that Data can be used to train or improve the AI tool. The following issues are central to understanding and addressing data rights. They are often introduced at a high level in an AI clause, but must be implemented through the data license and related provisions to be effective.

## Data Mapping

Each party must identify and map the Data that the AI tool accesses, processes, or generates, and track how and for what purpose that Data is used. AI may touch far more than clinical datasets. Examples include:

- protocols and informed consent documents
- trial systems such as EDC, CTMS, eTMF, and EHR platforms
- operational records and communications
- transcripts from ambient listening tools
- analyses of trial data or operational workflows

Personnel may inadvertently disclose Data by entering trial-related materials into AI tools that retain or transmit that information externally.

AI Data mapping should be treated as an ongoing exercise, not a one-time diligence task.

## Scope of Data Use

Contracts should clearly define the purposes for which the contracting party or its vendors may touch Data, keeping in mind that Data includes AI-generated outputs.

Key questions include:

- Is use of Data limited to performing the contracted services?
- May Data be used for internal analytics, product development, or other non-service purposes?
- May Data be used to train, refine, or improve the contracting party's or vendor's AI systems beyond the services being provided?
- Are heightened protections applied to sensitive data?
- What internal controls govern AI access to and use of Data?
- How does the contracting party control or restrict use of everyday AI tools?
- Is the use consistent with the parties' confidentiality obligations?

Where AI training or improvement is permitted, contracts should also clarify who benefits and how broadly Data may be used for those purposes.

For example, training or improvement may be subject to:

- **Siloed use:** Restricted to the services provided (i.e., "siloed" for the contracting party)
- **Vendor-, site- or sponsor-wide use:** Used to improve the vendor's platform for its customers or to support other trials conducted by the institution or sponsor
- **Broader AI use:** Used to improve the vendor's broader AI products

## De-Identified Data

To avoid siloing obligations, some vendors seek to use “de-identified” Data for secondary purposes such as model training, refinement or analytics. However, the meaning of de-identification can vary. For example, the HIPAA Safe Harbor method of de-identification requires removal of patient identifiers but not of sponsor names, study products, protocols, or other proprietary information. As a result, de-identified Data may still create competitive or intellectual property risks. Contracts should define what “de-identified” means, address removal of proprietary and trial-specific information, and clearly limit permitted downstream use.

## Data Retention and Deletion

Contracts should address how Data is handled by the AI tool after AI processing, including:

- whether Data inputs or outputs are retained
- deletion obligations
- post-termination obligations

Where AI systems are trained or fine-tuned using Data, complete deletion may not always be technically feasible.

## Commercial Exploitation Risk

AI tools may enable the contracting party or its vendors to extract insights from Data and use those insights to develop or enhance tools, datasets, or services beyond the contracted services. Without clear restrictions, this can result in one party monetizing value derived from Data generated at the other party’s expense. For example, AI insights may be used to identify biomarkers, develop predictive algorithms, inform future study design, or generate cross-study performance metrics offered to other customers.

In addition, use of AI systems without appropriate confidentiality, retention, and use restrictions may result in unintended disclosures that could start the clock on the U.S. one-year patent grace period or jeopardize patent rights in jurisdictions that require absolute novelty prior to filing.

**Takeaways:** The key issue is not whether AI is used, but how broadly Data is used by the AI tool and who benefits. Contracts should clearly define whether Data use is limited to the services or may be used more broadly, including for training or product improvement.

## III. Training Data

[Contract Clauses: Intellectual Property | Representations and Warranties | Audit | Indemnification | Limitation of Liability](#)

Organizations should evaluate:

- what data was used to train the AI system
- how that training data was obtained – by license, web scraping, or another method
- whether those acquisition methods were lawful
- whether the AI is being deployed in accordance with those rights

**Takeaway:** Training data provenance is a core risk area. Do not assume AI systems are trained on properly sourced data. Contracts should contain clear representations regarding acquisition and permitted use of training data, along with audit rights and appropriate allocation of liability.

## IV. Compliance and Regulatory Risk

**Contract Clauses:** [HIPAA](#) | [Informed Consent](#) | [Compliance with Applicable Laws](#) | [Representations and Warranties](#) | [Documentation](#) | [Recordkeeping](#) | [Audit](#) | [Indemnification](#)

AI use in clinical trials may implicate federal and state laws, including privacy, human subject protection, and FDA regulatory requirements.

### Patient Privacy and Human Subject Protection

For patient data, AI use may trigger processing or disclosure obligations under HIPAA and evolving state privacy, wiretapping and AI laws. For example:

- **HIPAA:** AI tools must comply with HIPAA when creating, receiving, maintaining and storing PHI.
- **Wiretapping:** State wiretapping laws may require patient consent before the use of ambient listening tools.
- **State Privacy and AI laws:** State privacy or AI laws may require disclosure of AI usage or consent by the patient.
- **Informed Consent:** the Informed consent regulations, including [45 CFR 46](#) and [21 CFR Part 50](#), require that subjects (participants) be provided with the information a reasonable person would want to have in order to make an informed decision about participation. While neither regulation explicitly addresses artificial intelligence, where AI is used in ways that could affect subject privacy, data integrity, or the reliability of study outputs, that use may be material to the patient's decision to participate, particularly if it introduces risks or uncertainties beyond those of conventional trial conduct.
- **Subject Safety:** AI use may also raise human subject protection considerations, including whether use of AI in trial operations could affect subject safety.

Contracting parties should assess whether the AI tool is designed and implemented to comply.

### FDA Regulatory Obligations

- **FDA Framework:** In January 2025, [FDA issued draft guidance](#) establishing a risk-based framework for AI used to produce information or data intended to support regulatory decision-making for drugs and biologics. The guidance applies to sponsors and "other interested parties," a term that is not defined. In practice, this may include contracting parties that use AI to generate information supporting regulatory decision-making. The draft guidance does not specifically address AI embedded in site-level tools, such as EHR systems, leaving uncertainty about how those uses should be evaluated where outputs may affect patient safety or the reliability of study results. For sponsors, this gap carries practical significance: FDA may evaluate how AI is used to generate or influence trial data during inspections or submission review, regardless of whether that AI sits with the sponsor, a

CRO, or a site.

- **Digital Health Technologies:** [FDA's December 2023 final guidance on digital health technologies used in clinical investigations](#) (DHT Guidance), which we wrote about [here](#) and [here](#), is addressed to sponsors, investigators and other stakeholders. The DHT Guidance requires that DHTs used to collect clinical trial data be fit for purpose and appropriately validated for their intended use. AI-enabled tools that function as DHTs, including ambient listening tools and AI-assisted documentation platforms whose outputs become part of the trial record, would be subject to these requirements. The guidance does not carve out an exception for tools characterized as operational.
- **GCP Oversight:** Sponsors retain oversight obligations under Good Clinical Practice (GCP). Even when AI tools are used by sites or vendors, sponsors remain responsible for trial conduct, including oversight of any CROs or vendors deploying AI-enabled systems on their behalf.
- **Inspections:** AI use may raise inspection readiness challenges. Sponsors and sites should be prepared to explain how AI tools are used, how outputs are validated, and how data integrity is maintained. FDA's BIMO inspectors expect personnel to understand the processes that generate trial records. If staff cannot explain the role of AI in generating or analyzing trial documentation, regulators may question the reliability of the underlying records.
- **Data integrity:** The parties should consider whether and how Data touched by AI is used in trial records and regulatory submissions, including whether investigators are required to attest to the accuracy of entries generated or modified by AI (e.g., in EDC) and whether sponsors rely on AI-generated (or impacted) outputs in submissions to regulatory authorities. FDA's ALCOA+ framework requires that records be attributable, legible, contemporaneous, original, and accurate; entries generated or modified by AI can create tension with several of these requirements, particularly attribution and originality.
- **Informed Consent:** See section above on Patient Disclosures and Consents.

## Audit and Cooperation

- **Audit Rights and Change Control:** Each party should retain the right to audit the other party's use of AI tools, including access to validation records, change logs, and model documentation, along with notice of material model changes, approval rights where AI tools touch regulated Data, and flow-down obligations to each party's vendors.
- **Regulatory Cooperation:** All parties and their vendors should be contractually obligated to support inspection readiness, including providing validation documentation and cooperating with FDA requests.

## Governance

Parties should also consider what oversight exists for AI use and whether the contracting party has an AI governance policy appropriate to the tool and the risks involved. Where no such policy exists, or where the policy does not specifically address use in regulated clinical trial activities, that gap itself represents a compliance risk.

**Takeaway:** Regulatory responsibility cannot be contracted away. Sponsors remain accountable for trial conduct regardless of how AI tools are deployed, and all parties should ensure that contracts reflect their compliance obligations, including audit rights, change control, and regulatory cooperation, before AI tools touch regulated Data or records.

## V. Cybersecurity

[Contract Clauses: Security](#) | [Indemnification](#) | [Limitation of Liability](#) | [Insurance](#)

- **Increased Vulnerability:** AI platforms expand the attack surface for clinical trial data. Vulnerabilities in AI systems

may also create indirect entry points into sponsor or site environments if security architecture and access controls are not properly implemented.

- **Data Leakage:** AI systems may also introduce data leakage risks, particularly where platforms retain inputs, transmit data externally, or operate within multi-tenant environments. Similar risks arise when personnel enter trial materials into consumer AI tools outside of controlled systems.
- **Security Controls:** Organizations should assess vendor security standards, certifications, audit rights, and incident response procedures, including breach notification obligations.

## VI. Monitoring and Validation

Contract Clauses: AI | Oversight and Monitoring | Representations and Warranties | Subject Injury

Organizations should evaluate:

- whether the AI tool has been validated for accuracy and reliability
- mechanisms to detect and remediate bias or performance issues
- whether and when human review is required
- what ongoing oversight exists for AI use, including monitoring, validation, and escalation procedures
- whether contracts require periodic revalidation and updates to the AI tool

These considerations are particularly important where AI outputs are incorporated into trial records or relied upon in analyses, as failures in validation or oversight may not become apparent until later stages of monitoring or inspection, and in some cases may affect subject safety.

Operational risks include:

- hallucinated or inaccurate content affecting clinical trial operations or incorporated into study records, safety narratives, or other trial documentation
- AI-generated content lacking audit trails
- errors propagating into regulatory submissions if outputs are not appropriately reviewed

Where addressed, AI clauses may require human review or validation at a high level, but these obligations should be supported by specific monitoring, validation, and audit provisions.

## VII. Risk Allocation

Contract Clauses: Representations and Warranties | Indemnification | Subject Injury | Insurance | Limitation of Liability | Cybersecurity

Contracts should address how AI-related risks are allocated between the parties, including careful consideration of:

- **Representations and warranties** relating to model performance, data provenance, intellectual property and vendor oversight
- **Responsibility for errors for AI-generated output:** Investigators, monitors or other personnel who may sign or approve AI-generated narratives, deviation assessments, or monitoring reports remain responsible for the accuracy of those documents. Approval implies verification, so relying on AI output without adequate independent review may itself constitute a failure of oversight, compounding liability for any inaccuracies contained in the underlying record. Contracts should clearly allocate responsibility for AI-generated errors between sponsors, sites, and vendors

- **Indemnification** for data privacy and security violations, bias claims, use of Data by the contracting party and its vendors, and intellectual property infringement and, where appropriate, claims arising from AI-related impact on trial conduct or subject safety
- **Subject injury:** Contracts should address whether and to what extent injuries arising from the use of AI in trial operations are covered under subject injury provisions, including where AI-related errors or failures contribute to protocol deviations, operational decisions, or other conduct affecting subject safety
- **Insurance** coverage supporting the indemnification obligations, including AI-specific risks and potential subject injury exposure from operational AI use. Organizations should review their cyber policy coverage for AI exclusions
- **Liability exclusions and caps:** These should account for AI-related risks, including HIPAA and state law violations, competitive injury, intellectual property, hallucinations, bias, and subject injury. Separate caps may be appropriate for certain AI-related risks.
- **Cross-clause and contract coordination:** Indemnification, insurance and liability provisions should align internally and with upstream and downstream contracts. AI, data use and cybersecurity should also be drafted with these relationships in mind.

**Takeaway:** AI does not shift responsibility. Contracts must clearly allocate risk for AI-generated outputs, including who is responsible for inaccuracies and any resulting effects on trial conduct or subject safety, and how those risks are supported through indemnification, subject injury, insurance, and liability provisions.

## VIII. Conclusion

AI is already embedded in many tools used to run clinical trials, often without organizations realizing it. As a result, contracts, diligence practices, and governance frameworks must evolve to address the risks created by AI-enabled technologies.

The regulatory framework governing clinical trial conduct, industry norms, and technology law are only beginning to address AI-specific risks, making contracts, diligence, and governance frameworks the primary tools available to manage them today. FDA's draft guidance on AI used to support regulatory decision-making is a meaningful step, and FDA's DHT Guidance reinforces existing expectations for tools that capture clinical trial data. However, neither guidance fully resolves how AI embedded in trial operations – particularly at site and vendor levels – should be evaluated where its outputs may affect patient safety or the reliability of clinical trial results, or how the expectations will be applied in practice.

The issues outlined in this series are not exhaustive, and the landscape will continue to evolve. Organizations that ask the right questions – of their contracting partners, their vendors, and themselves – will be better positioned to deploy AI responsibly, protect the integrity of trial data, and meet their regulatory obligations.

Ultimately, deploying AI does not transfer responsibility. Sponsors, sites, and vendors remain accountable for how AI systems interact with clinical trial data and for the integrity of the records those systems help produce.



If you have any questions or would like more information about these developing issues, please contact the following:

**KATHERINE LEIBOWITZ**

**1-610-896-5788**

**[Katherine.Leibowitz@LeibowitzLawTeam.com](mailto:Katherine.Leibowitz@LeibowitzLawTeam.com)**