AI DATA GOVERNANCE IN HEALTHCARE

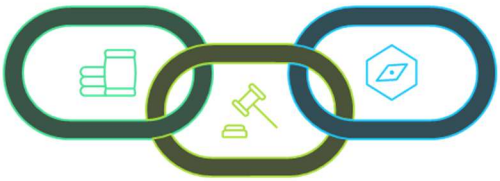
AI Secondary Use, Model Training & Data Sovereignty Provisions

Contract Language Reference

Standard boilerplate provisions and AI-specific addendums for healthcare contracts.

Core Governance Principle

The fundamental principle guiding AI data governance in healthcare.



Regulatory Basis

Mandatory regulatory language and compliance requirements for AI data

Summary & Purpose:

Every week, thoughtful posts circulate about how AI oversight should take shape. The dominant posture treats AI development as operating in a kind of regulatory white space or as a domain needing its own rules.

Regulations are technology agnostic. Technology is not a regulated subject. It does not matter whether the processing is a query, report, model, or inference engine. Obligations address use, who uses it, when they use it, how they use it and why.

Healthcare operations under *HIPAA §164.501* cover quality assessment, care coordination, clinical training, and certain population-based activities for the covered entity's own purposes. Training a model that will be productized, licensed, or sold is not healthcare operations for the originating entity.

The real reason "AI Pilots Fail"

What vendors call pilots, health systems and health plans call proof of concept.

Standard scenario: a vendor and a health plan align on an AI use case, run a POC, generate impressive results and then legal and compliance review reveals that the existing BAA, DUA, and SOW never authorized the data use.

- The POC cannot move to production.
- The data used in the pilot may have been processed outside authorized scope.
- The remediation is expensive, timelines collapse, and relationships strain.

I once took over a $500M M&A due diligence where technical incompatibilities were tabled because it was expected they "could be resolved in design". I knew the risk, required the analysis and it would have been a **$58M sunk cost addition with a minimum of 12 months for readiness to scale.**

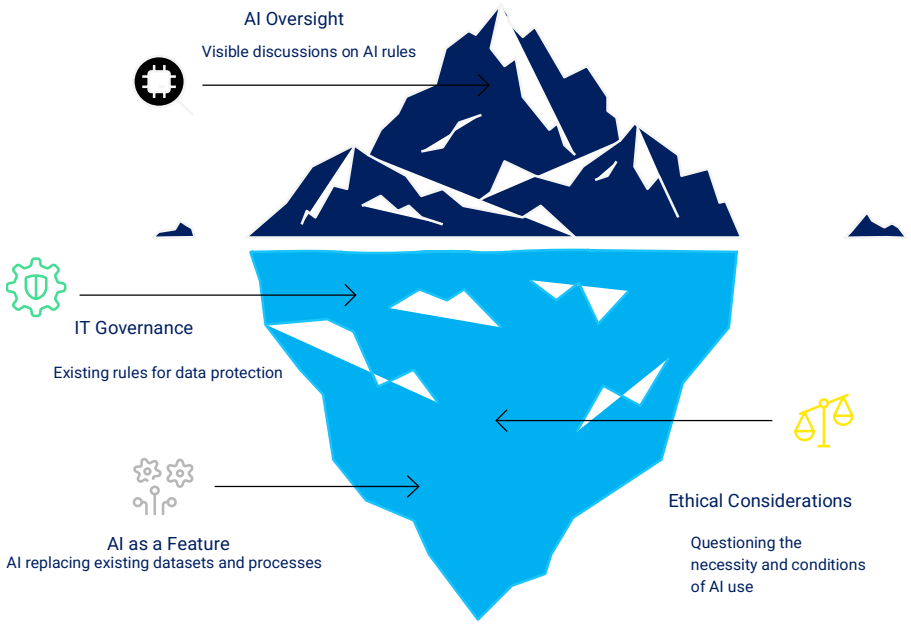
Myth: *"It's our EDW. It's de-identified. It's aggregate. We can use it for AI dev."*

Reality: De-identification is a process, not a permanent state. Model outputs can re-identify individuals even when trained on data that passed Safe Harbor methodology. Expert Determination is required for each processing modality, including AI models.

Myth: *"AI is new, so the regulations are unclear, so we have flexibility."*

Reality: HIPAA's framework is technology-neutral by design. OCR has confirmed explicitly. The novelty is in the use case, not rules. AI's capacity to infer, generalize, and retain creates risk exposure in existing frameworks.

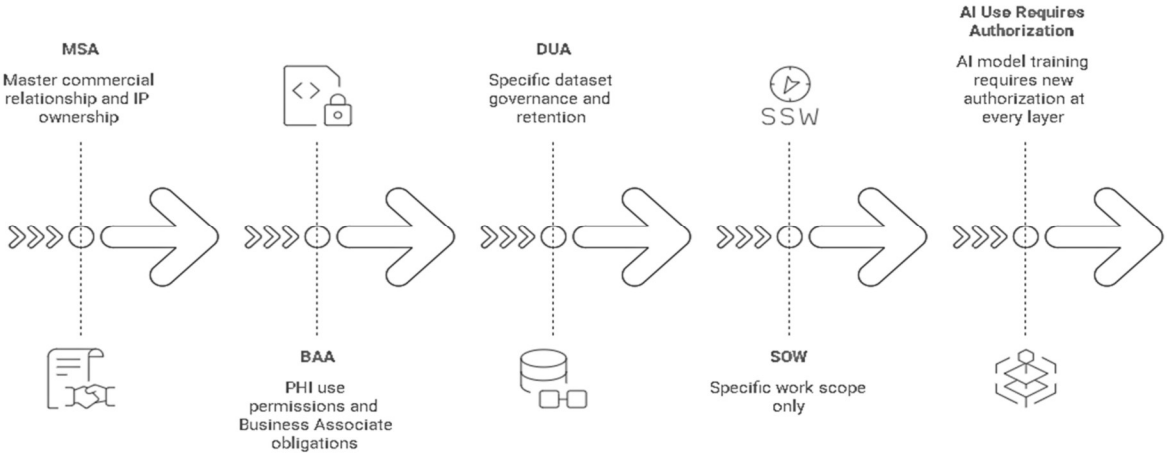
AI Governance: Beyond the Surface



PART 1 DATA SOVEREIGNTY

1.1 The Covenant Chain

Healthcare data governance operates through four interlocking instruments. Each narrows the permissible universe of data use established by the layer above it. A vendor cannot acquire rights at a lower layer that were not granted at a higher one. AI readiness means ensuring prior authorization is complete at every.

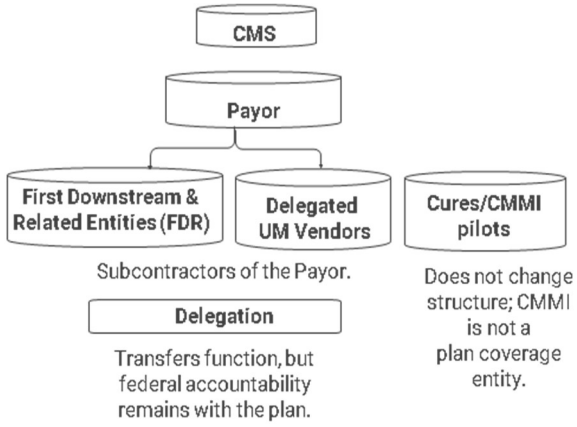


	Primary Function	AI-Relevant Scope
MSA	Master commercial relationship; IP ownership; master data use	Must address secondary use prohibition; model weight ownership; product development restriction
BAA	PHI-specific use/disclosure permissions; Business Associate obligations under HIPAA	Must enumerate AI permitted uses explicitly — training, inference, and aggregation are not implied by service delivery language
DUA	Governs specific datasets; transfer mechanisms; retention and destruction schedules	Must specify whether data may be used for model training; synthetic data generation; derived asset ownership

	Primary Function	AI-Relevant Scope
SOW	Scopes specific deliverables the necessary work and data use	Each AI engagement (pilot, POC, live)requires its own SOW; POC auth does not carry forward to prod

1.2 The Data Sovereignty Hierarchy

Rights flow downward through the delegation chain and cannot be expanded at lower levels. Understanding this hierarchy is essential.



Structural Reality of Contracting

- Payors are the only entity directly contracted with CMS.
- First Downstream & Related Entities(FDR) and delegated UM vendors are subcontractors
- Vendors in Cures/CMMI pilots do not change structure, CMMI is not a coverage entity.
- Delegation transfers function. Federal accountability remains with the plan.
- FDR must satisfy HIPAA + FDR requirements. The plan is accountable for both.

Layer	Rights & Obligations	AI Implication
Individual Member/ Patient	Fundamental rights under HIPAA, state privacy law, consent frameworks not severable	Cannot be waived by CE or BA on the individual's behalf; state specific opt-out rights emerging
Covered Entity	Custodian, not absolute owner. SaaS vendors and FDRs are not exempt from this structure.	Cannot grant rights it does not have; cannot authorize secondary use without individual notice mechanisms
Business Associate	Delegated, scoped, purpose-limited processing rights per BAA; cannot exceed CE grant; cannot sub-delegate w/o auth	Model weights derived from CE data are a derived data asset — BA cannot retain after contract termination without explicit written authorization
Sub-BA / SaaS / AI Vendor	Each delegation narrows further; a sub-BA agreement cannot permit uses the BA agreement prohibits	AI product development, cross-client data aggregation, and federated learning all require explicit authorization at every layer above

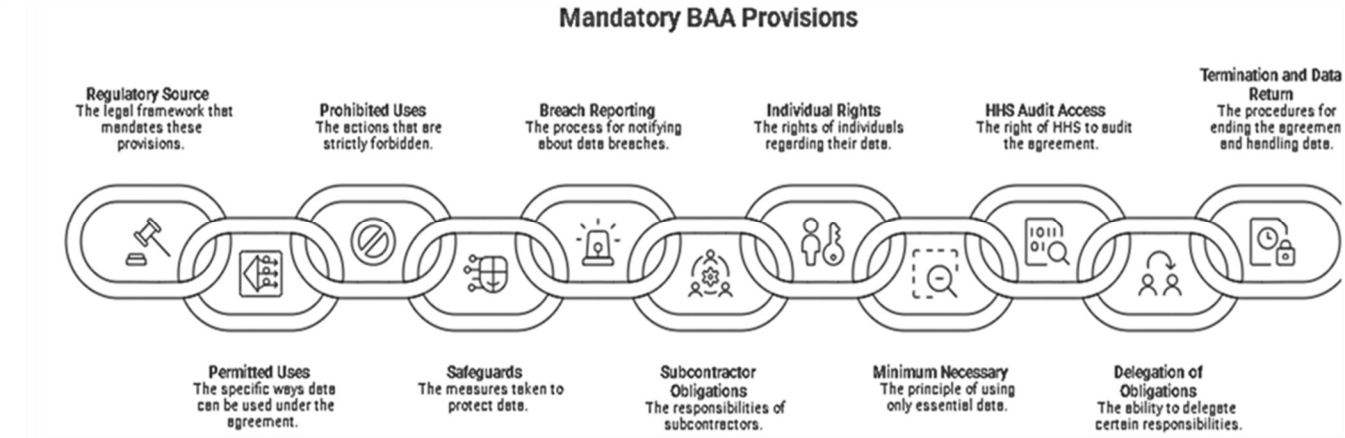
1.3 Secondary Use: The Defined Boundary

Secondary use of healthcare data is a defined legal concept. Data collected for Purpose A cannot be repurposed for Purpose B without independent authorization.

Original Authorized Use	Attempted Secondary Use	Status
Claims analytics for utilization management	Training a prior authorization AI model	Addendum required before any use
Quality measurement (HEDIS/Stars)	Building a risk stratification product	Addendum required before any use
Care management platform data	Federated model training across clients	Likely BAA breach; cross-client commingling prohibited
EDW population health reporting	Vendor AI product development	Secondary use violation; requires independent authorization

Original Authorized Use	Attempted Secondary Use	Status
POC/pilot w/ real PHI	Productizing outputs without new authorization	Retroactively problematic; POC SOW does not authorize production

PART 2 BUSINESS ASSOCIATE AGREEMENT (BAA)



2.1 Mandatory Provisions — 45 CFR § 164.504(e)(2)

The following provisions are boilerplate and illustrative of required elements. If they are absent the agreement non-compliant and is equivalent to having no BAA at all. However, if they are silent or omitted, it does not relieve the BA from those duties as these are plan requirements, BA must annually attest compliance.

2.1.1 Permitted Uses and Disclosures (Required — Non-Negotiable)

> Business Associate may only use or disclose Protected Health Information as necessary to perform the services set forth [Service Agreement/Exhibit], and for no other purpose.

Implementation note: 'As necessary to perform services' is the minimum threshold. For AI engagements, the SOW and this clause must enumerate permitted processing modalities explicitly. Absence of enumeration equals absence of permission.

2.1.2 Prohibition on Non-Permitted Uses (Required)

> Business Associate shall not use or disclose Protected Health Information in a manner that would violate the requirements of 45 CFR Part 164, Subpart E, if done by Covered Entity, except as permitted under Sections [X] and [Y] of this Agreement.

2.1.3 Safeguards (Required)

> Business Associate shall implement appropriate administrative, technical, and physical safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement and shall comply with Subpart C of 45 CFR Part 164 (Security Rule) with respect to electronic Protected Health Information.

2.1.4 Breach and Incident Reporting (Required)

> Business Associate shall report to Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware, without unreasonable delay and in no case later than [60 / 30 / 5] calendar days after discovery.

Note: 60 days is the regulatory floor. Well-negotiated BAAs often compress this to 30 or 5 days. AI systems with automated processing pipelines warrant shorter windows given the complexity of discovery in model environments.

2.1.5 Subcontractor Obligations (Required — HITECH 2013)

> Business Associate shall ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate, by entering into a written agreement that complies with 45 CFR 164.504(e).

> Business Associate shall not authorize any Subcontractor to use or disclose Protected Health Information in a manner that would not be permissible under this Agreement if done by Business Associate.

2.1.6 Individual Rights Support (Required)

> Business Associate shall make available Protected Health Information in a designated record set to Covered Entity as necessary to satisfy obligations under 45 CFR 164.524 (access), 164.526 (amendment), and 164.528 (accounting of disclosures).

2.1.7 Minimum Necessary (Embedded Obligation)

> Business Associate shall make reasonable efforts to use, disclose, and request only the minimum amount of Protected Health Information necessary to accomplish the intended purpose, consistent with 45 CFR 164.502(b) and 164.514(d).

2.1.8 HHS Audit Access (Required)

> Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of HHS for purposes of determining Covered Entity's compliance with the HIPAA Rules.

2.1.9 Delegation of CE Obligations (Required — 45 CFR 164.504(e)(2)(ii)(H))

> To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to the performance of such obligation(s).

If **HIPAA obligations are delegated**, the CE remains liable for the BA's failure to perform. Delegation transfers function and not accountability. However, regulations require a BAA and contractual language. A BA must attest to compliance, be registered and follow mandates as standard in any contract. The absence of regulatory clauses are not carve outs.

2.1.10 Termination and Data Return/Destruction (Required)

> Upon termination of this Agreement, Business Associate shall return or destroy all Protected Health Information received from, or created on behalf of, Covered Entity. Business Associate shall not retain copies. Where return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to retained information and limit further uses to those purposes that make return or destruction infeasible.

2.2 AI-Specific BAA Provisions (Addendum Required)

The following provisions are not in HHS sample language. They are required when AI model development, training, inference, or productization is contemplated. A BAA addendum must be executed before any AI use of PHI begins not a retro correction.

2.2.1 Use Enumeration

> uses of PHI for Artificial Intelligence purposes [PERMITTED / NOT PERMITTED]:
> (a) Use of PHI to train, fine-tune, or validate ML models -Depends
> (b) PHI in automated inference pipelines with outputs stored beyond SOW term - No
> (c) Aggregation of PHI with other CE clients' data for model training - No
> (d) De-identified data derived from PHI for AI model training – Yes 45CFR 164.514(b)
> (e) Retention of model weights or parameters derived from PHI post-termination - No
> (f) PHI-derived synthetic data for product development – per SOW

2.2.2 Model Weight and Derived Asset Ownership

> Any ML model, model weights, embeddings, or other derived computational artifacts created using PHI or data derived therefrom shall be the sole property of Covered Entity [or jointly owned per Exhibit X. Business Associate shall not retain, commercialize, license, or transfer such derived assets following termination. Upon termination, XX shall certify destruction of all such assets within [30] days.

2.2.3 Cross-Client Data Prohibition

> Business Associate shall not combine, aggregate, or commingle PHI received from Covered Entity with PHI from any other covered entity client for purposes of AI model training, product development, or any other purpose, without Covered Entity's prior

written consent and execution of a written amendment to this Agreement.

2.2.4 Secondary Use Prohibition and Notice Requirement

Business Associate shall not use any client data for any purpose beyond the SOW scope without: (i) written request at least [30] days in advance; (ii) obtaining Covered Entity's prior written consent; and (iii) executing a written amendment. No secondary use is authorized by implication, course of conduct, or prior practice.

2.2.5 AI Subprocessor Disclosure

Business Associate shall provide a complete list of all Subcontractors with access to PHI in connection with AI processing, within [60] business days of addition or change. Covered Entity may object within [30] business days. Business Associate shall not engage a new AI Subcontractor in the event of documented objection.

PART 3 — MASTER SERVICES AGREEMENT (MSA)

3.1 Standard Data Use and IP Provisions

The MSA establishes the master commercial framework governing all SOWs and BAAs executed under it. AI readiness at the MSA level is non-negotiable — SOW-level restrictions are insufficient if the MSA grants broader rights that override them.

3.1.1 Data Ownership and License Grant

All data provided by Client to Vendor, including PHI, de-identified data, aggregate data, metadata, remains the sole and exclusive property of Client. Vendor receives a limited, non-exclusive, non-transferable license to use Client Data solely to perform services described in applicable Statements of Work. No other use is authorized.

3.1.2 Prohibition on Secondary Use

Vendor shall not use Client Data for any purpose other than performance of the applicable SOW, including but not limited to: (a) development, training, validation, or improvement of Vendor's products or services; (b) development or training of AI or ML models; (c) benchmarking or market research; (d) services to third parties; or (e) any commercial purpose not explicitly authorized in the applicable SOW. This prohibition applies regardless of whether Client Data has been de-identified, aggregated, or transformed.

3.1.3 AI and Machine Learning Specific Restrictions

Notwithstanding any other provision, Vendor shall not: (a) use Client Data to train, fine-tune, test, or validate any AI, ML, or large language model without Client's prior written consent and an executed AI Data Use Addendum; (b) include Client Data or derivatives in any dataset used to develop products for parties other than Client; (c) retain model weights, embeddings, or computational artifacts derived from Client Data beyond the term of the applicable SOW.

3.1.4 Notification and Amendment Requirement for New Uses

Vendor shall provide Client no less than [30] days' written notice before implementing any material change to technology, processing methods, subprocessors, or data use practices. 'Material change' includes: introduction of AI/ML processing; change of AI or cloud infrastructure; addition of automated decision-making; any change altering the risk posture of data processing. Client may reject any such change within [15] days; Vendor shall not implement a rejected change without Client's written consent.

3.1.5 Intellectual Property — Work Product and Derived Assets

All work product, deliverables, analyses, reports, and models created by Vendor specifically for Client shall be the sole property of Client upon payment. Vendor retains pre-existing IP and general methodologies. Any ML model or computational artifact developed using Client Data as a material input shall be deemed work product owned by Client [or subject to joint ownership terms in Exhibit __].

3.1.6 Technology Introduction Review Requirement

Introduction or replacement of any technology that materially affects the risk posture of Client Data processing requires, prior to implementation: (a) written notice to Client; (b) Client's written approval; (c) an updated risk assessment; (d) amendment of

> BAA and DUA as necessary; and (e) review by Client's Legal, Compliance, and (where applicable)Actuarial functions. Vendor assumes responsibility for non-compliance resulting from technology changes made without completing this process.

PART 4 — DATA USE AGREEMENT (DUA)

4.1 Core DUA Provisions

A Data Use Agreement governs specific data sets, particularly limited data sets under 45 CFR 164.514(e) and de-identified data. DUAs must be dataset-specific and purpose-specific. A DUA authorizing analytics does not authorize AI model training on the same dataset, even if the underlying data is nominally de-identified.

4.1.1 Data Set Description and Purpose Limitation

> This DUA governs the following data set: [Description, source system, date range, fields included, record count estimate]. Permitted uses are strictly limited to: [e.g., population health analytics, quality measurement, care gap reporting]. No other use is authorized, including ML model training, product development, or provision of services to third parties.

4.1.2 De-identification Standard

> Data represented as de-identified has been processed in accordance with: [OPTION A: Safe Harbor under 45 CFR 164.514(b)(2), with removal of 18 specified identifiers] / [OPTION B: Expert Determination under 45 CFR 164.514(b)(1), certified by [Qualified Expert, Credential], dated [Date], on file]. Recipient agrees not to attempt re-identification of any individual.

! Prior de-identification certifications do not extend to new processing modalities. AI model training on 'de-identified' data requires a new Expert Determination. AI inference creates re-identification risks that Safe Harbor methodology was not designed to address. ML models can embed re-identifiable patterns from data that passed Safe Harbor. This is not a theoretical risk; it is a recognized threat vector with documented methodology.

4.1.3 Retention and Destruction

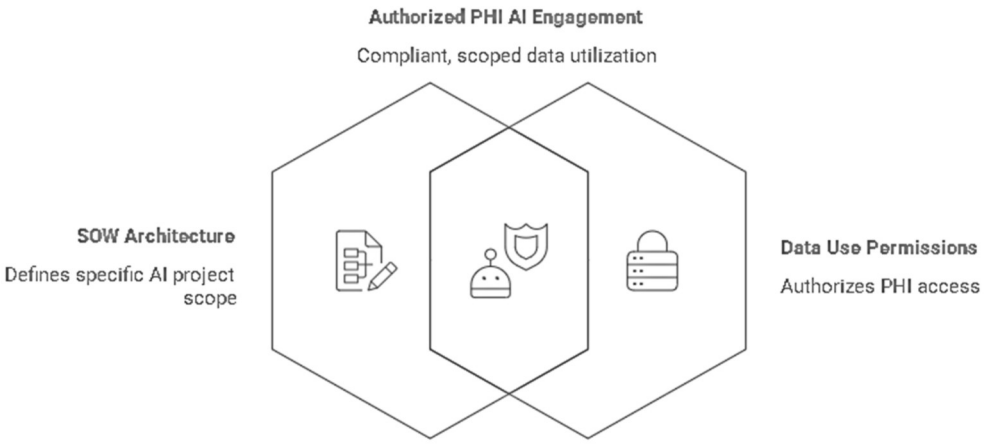
> Recipient shall retain the Data Set only for the period necessary to accomplish Permitted Uses, and no longer than [Term]. Upon expiration or completion of Permitted Uses, whichever is earlier, Recipient shall destroy all copies and derivatives — including analytical outputs, model training sets, and computational artifacts — and provide written certification of destruction within [15] business days.

4.1.4 Subrecipient Requirements

> Recipient shall not disclose the Data Set to any subrecipient without prior written consent. Any authorized subrecipient must execute a written agreement imposing the same restrictions. Recipient remains jointly and severally liable for non-compliance.

4.1.5 AI Model Training Prohibition / Authorization

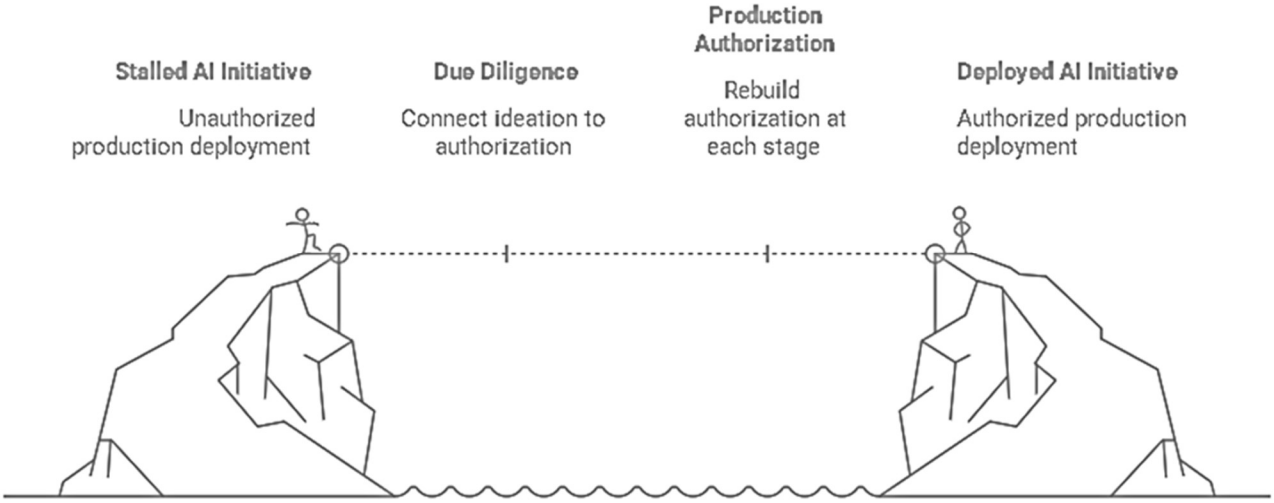
> [PROHIBITION] Recipient shall not use the Data Set or any derivative for training, fine-tuning, testing, or validating any AI, ML, predictive analytics, or automated decision-making model without prior written consent and written AI Data Use Addendum.
>
> [AUTHORIZATION — where AI training is permitted] Recipient is authorized to use the Data Set for training the following specific model: [description, purpose, architecture scope]. No other AI use is authorized. Model weights and derived artifacts remain subject to Section [X — IP/ownership].



PART 5 — STATEMENT OF WORK (SOW)

5.1 SOW Architecture for AI Engagements

The SOW is the most granular permission instrument. It scopes the specific work the data can support — and nothing beyond it. Every AI engagement requires its own SOW. A POC SOW does not authorize production. A pilot SOW does not authorize model productization. Real PHI used in a POC requires a PHI-scoped SOW even if the eventual production system will operate on de-identified data.



5.1.1 Scope and Data Specification

> This SOW authorizes Vendor to perform the following services: [Enumerated description].Data authorized under this SOW is limited to: [Data set, source systems, date range, record population, specific fields]. Any data use not described here requires a written SOW amendment prior to implementation.

5.1.2 AI/ML Use Limitations

> AI or ML processing under this SOW is limited to[Specific model type, inference purpose, output type]. Vendor shall not:(a)use data from this SOW to train or improve models used for services to other clients;(b)retain model outputs, scores, or predictions beyond [retention];(c)incorporate data from this SOW into any general-purpose or foundation model.

5.1.3 Pilot / POC Specific Provisions

> This SOW authorizes a time-limited proof of concept ('POC') for: [evaluation objective]. The POC is limited to the data set, time period, and user population described herein. POC outputs — including model training data, validation results, benchmarks, and derived insights — are the property of Client. Vendor shall not use

> POC outputs for commercial proposals, product development, or services to third parties without Client's written consent. This SOW does not constitute approval for production deployment; production requires execution of a separate SOW and, where applicable, updated BAA and DUA.

5.1.4 Acceptance Criteria and Review Triggers

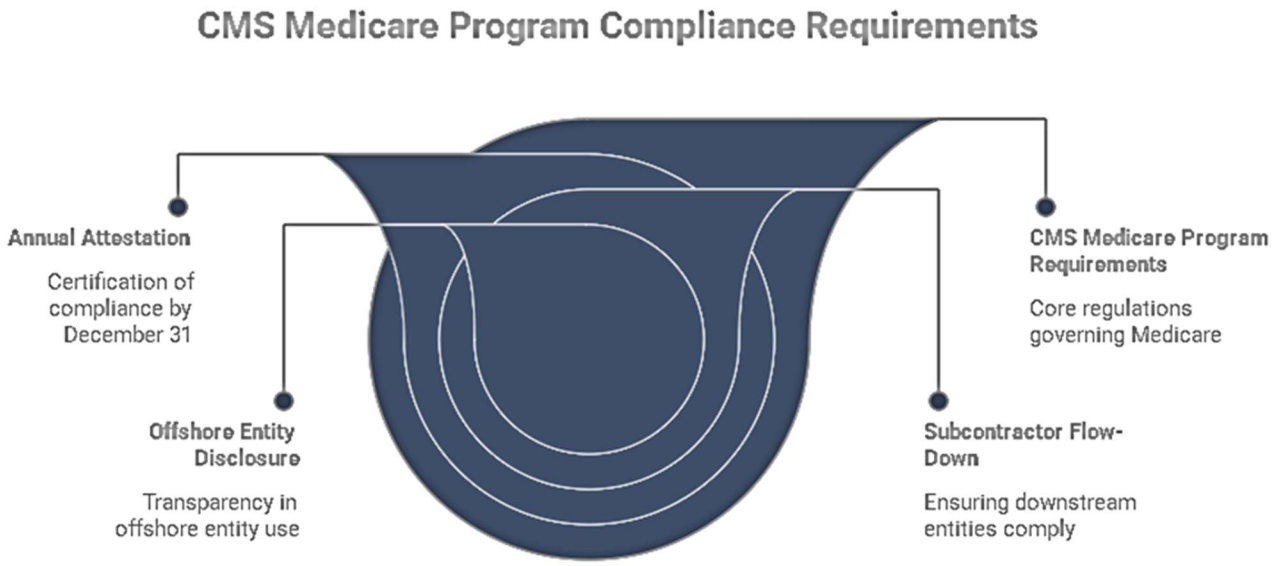
> Where services include automated decision support for UM, risk stratification, benefit determination, or claims adjudication, Client acceptance is conditioned on satisfactory completion of: (a) Legal review of decision logic; (b) Compliance review against HIPAA,CMS, and accreditation standards; (c) Actuarial review of impact on pricing assumptions and regulatory filings. Vendor shall provide model explainability reports and audit trails sufficient to support these reviews.

PART 6 MEDICARE ADVANTAGE MANDATORY CONTRACT LANGUAGE

6.1 Regulatory Foundation

Medicare Advantage organizations are required under 42 CFR § 422.504(i) to flow specific CMS contractual requirements down to all First Tier, Downstream, and Related Entities. These are mandatory floor requirements — they are not negotiable, cannot be modified by contract, and cannot be waived. Non-compliance by an FDR is the plan's non-compliance with CMS.

> **42 CFR § 422.504(i)(1) Accountability Principle** MA organization maintains ultimate responsibility for adhering to and fully complying with all terms and conditions of its contract with CMS, notwithstanding any relationship(s) that the MA organization may have with first tier, downstream, and related entities. Delegation only transfers function.



6.2 FDR Definitions Regulatory Text

Entity	Regulatory Definition (42 CFR § 422.500 / 423.501)
First Tier Entity	Any party that enters into a written arrangement, acceptable to CMS, with an MA organization or applicant to provide administrative services or healthcare services to a Medicare eligible individual under the MA program.
Downstream Entity	Any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit, below the level of the arrangement between an MA organization and a first-tier entity. These arrangements continue down to the level of the ultimate provider of both health and administrative services.

Entity	Regulatory Definition (42 CFR § 422.500 / 423.501)
Related Entity	Any entity related to the MA organization by common ownership or control that:(1)performs some of the MA organization's management functions under contract or delegation;(2)furnishes services to Medicare enrollees under an oral or written agreement; or(3) leases real property or sells materials to the MA organization at a cost of more than $2,500 during a contract period.

6.3 Mandatory Contract Provisions 42 CFR § 422.504(i)(3) and (4)

All contracts between MA organizations and FDRs must contain the following. Plans may impose additional requirements but cannot reduce these.

6.3.1 HHS/Comptroller General Audit Rights (Mandatory)

> [FDR] agrees that HHS, the Comptroller General, or their designees have the right to audit, evaluate, collect, and inspect any books, contracts, computer or other electronic systems, including medical records, related to CMS's contract with the MA organization. This right applies during the term and for 10 years from the final contract date or completion of any audit, whichever is later. [42 C.F.R. §§ 422.504(i)(2)(i) and (ii)]

6.3.2 Confidentiality and Enrollee Record Accuracy (Mandatory)

> [FDR] shall comply with confidentiality and enrollee record accuracy requirements, including: (1) abiding by all Federal and State laws on confidentiality and disclosure;(2) releasing medical information only as permitted by law or court order; (3) maintaining records that are accurate, complete, and timely; and (4) giving enrollees access to records in accordance with applicable law.

6.3.3 Delegation Specification and Performance Monitoring (Mandatory)

> Each delegating contract shall: (i) specify delegated activities and reporting responsibilities with particularity; (ii) provide for revocation or other remedies if CMS or the MA organization determines performance is unsatisfactory; (iii) specify that performance is monitored by the MA organization on an ongoing basis;and (iv) specify review of credentials of affiliated medical professionals. [42 C.F.R. § 422.504(i)(4)]

6.3.4 Enrollee Protection Provisions (Mandatory)

> [FDR] agrees not to hold enrollees liable for payment of fees that are the obligation of the MA organization, consistent with 42 C.F.R. § 422.504(g)(1). This protection shall be included in all provider agreements and survives termination with respect to services rendered during the term.

6.3.5 Compliance Program Requirements (Mandatory)

> [First Tier Entity] shall maintain an effective compliance program per 42 C.F.R. §422.503(b)(4)(vi) and CMS Medicare Managed Care Manual, Ch. 21, including: (a)written standards of conduct and compliance policies;(b)compliance and FWA training within 90 days of hire and annually; (c)non-retaliation reporting mechanisms;(d)internal monitoring/auditing procedures;(e)corrective action procedures.

6.3.6 Fraud, Waste and Abuse Training (Mandatory)

> [First Tier Entity] shall ensure all employees and downstream entities complete General Compliance and FWA training: (a) within 90 days of hire or contracting; (b) upon material revision; and (c) annually. Records of completion shall be maintained for no less than 10 years and produced upon request by MA Plan or CMS.

6.3.7 Exclusion List Screening (Mandatory)

> [First Tier Entity] shall screen all employees, contractors, and downstream entities against: (a) HHS OIG LEIE; (b) GSA SAM; (c) CMS Preclusion List; and (d) applicable State exclusion lists. Screening shall occur prior to hire/contracting and monthly thereafter. Any excluded individual shall be immediately removed from Medicare-related work and [MA Organization] notified.

6.3.8 Offshore Entity Disclosure (Mandatory)

> [First Tier Entity] shall notify [MA Organization] in writing, in advance, of any use of an offshore individual or entity. Where offshore functions involve PHI,[First Tier

> Entity]acknowledges that [MA Organization] must submit a CMS attestation. [First Tier Entity] shall not engage an offshore entity w/o prior written approval.

6.3.9 Subcontractor Flow-Down (Mandatory)

> [First Tier Entity] shall require all Downstream Entities to comply with all applicable CMS Medicare program requirements, including but not limited to the requirements in this Agreement. [First Tier Entity] remains responsible for the compliance of all Downstream Entities and shall include equivalent provisions in all downstream agreements.

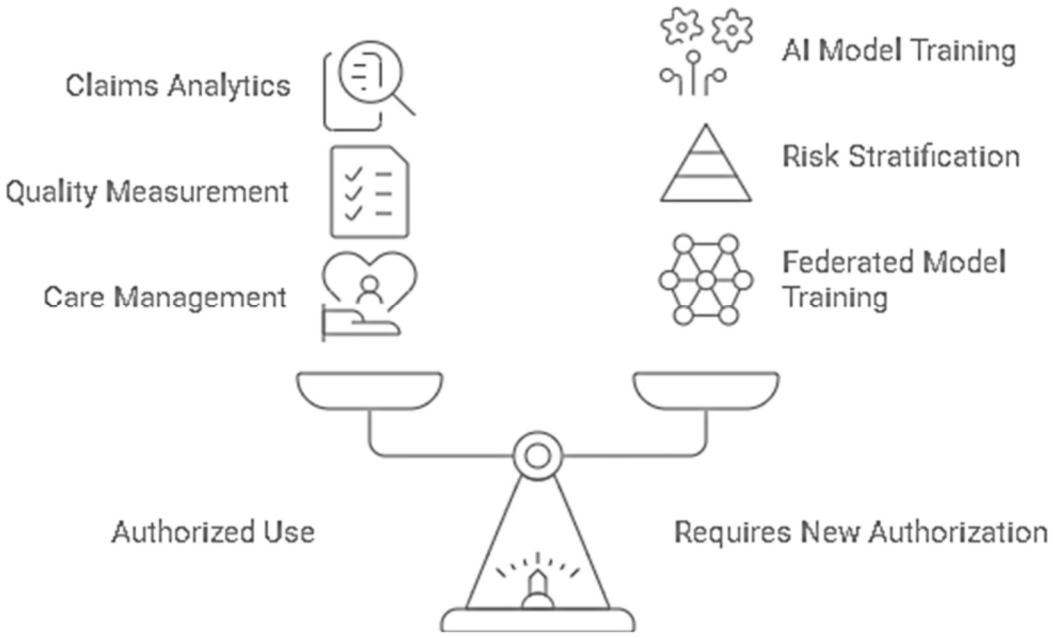
6.3.10 Annual Attestation (Mandatory)

> [First Tier Entity] shall complete and return [MA Organization]'s annual FDR attestation by [December 31] each contract year, certifying compliance with all applicable CMS requirements. Failure to complete the required attestation may result in corrective action up to and including contract termination.

PART 7 — AI DATA USE ADDENDUM FRAMEWORK

7.1 When an AI Addendum is Required

An Data Use Addendum to the MSA, BAA, and/or DUA is required before any of the following activities may commence. Existing agreements do not authorize these uses.



Triggering Activity	Addendum Req	Instruments
AI model training using client PHI	Before use	BAA + DUA +SOW
AI training on derived de-identified data	+new Detrmine	DUA + SOW
Pilot / POC using PHI or limited data set	Before access	BAA +DUA + SOW
Introduction of AI subprocessor or AI cloud	+new risk assess	MSA + BAA
AI-driven automated decision-making	+ legal/actuary	MSA +BAA + SOW
Federated learning across client populations	From each client	BAA + DUA
LLM/GenAI accessing PHI via RAG or fine-tuning	New risk analy	BAA + DUA +SOW
Retention of model weights post-contract term	Not permissible	MSA + BAA

7.2 Notice and Opt-Out Framework

New and secondary data uses require, at minimum, notification from the client and often the invite to opt out. Security and privacy notices must be updated and redistributed consistently with HIPAA NPP material change requirements.

Use Category	Default Posture	Notice Requirement	Consent Standard
AI model training on client PHI	OPT-IN required	30-day advance written notice	Affirmative written consent + addendum
Training derived/ de-identified data	OPT-IN required	30-day advance written notice	Written consent + new Expert Determination
Cross-client data aggregation	PROHIBITED absent authorization	Authorization required each CE	Written consent from each CE + addendum
AI subprocessor introduction	Notice required	10 business days advance notice	Right to object within 15 business days
AI-driven decision support (UM/claims)	Legal/actuarial review required	Notice + review period before live	Written approval post-review
Service improve/ model refine	Opt-out may be acceptable	Notice with opt-out window	Silence is not consent; opt-out must be real

7.3 NPP Material Change Update Obligation

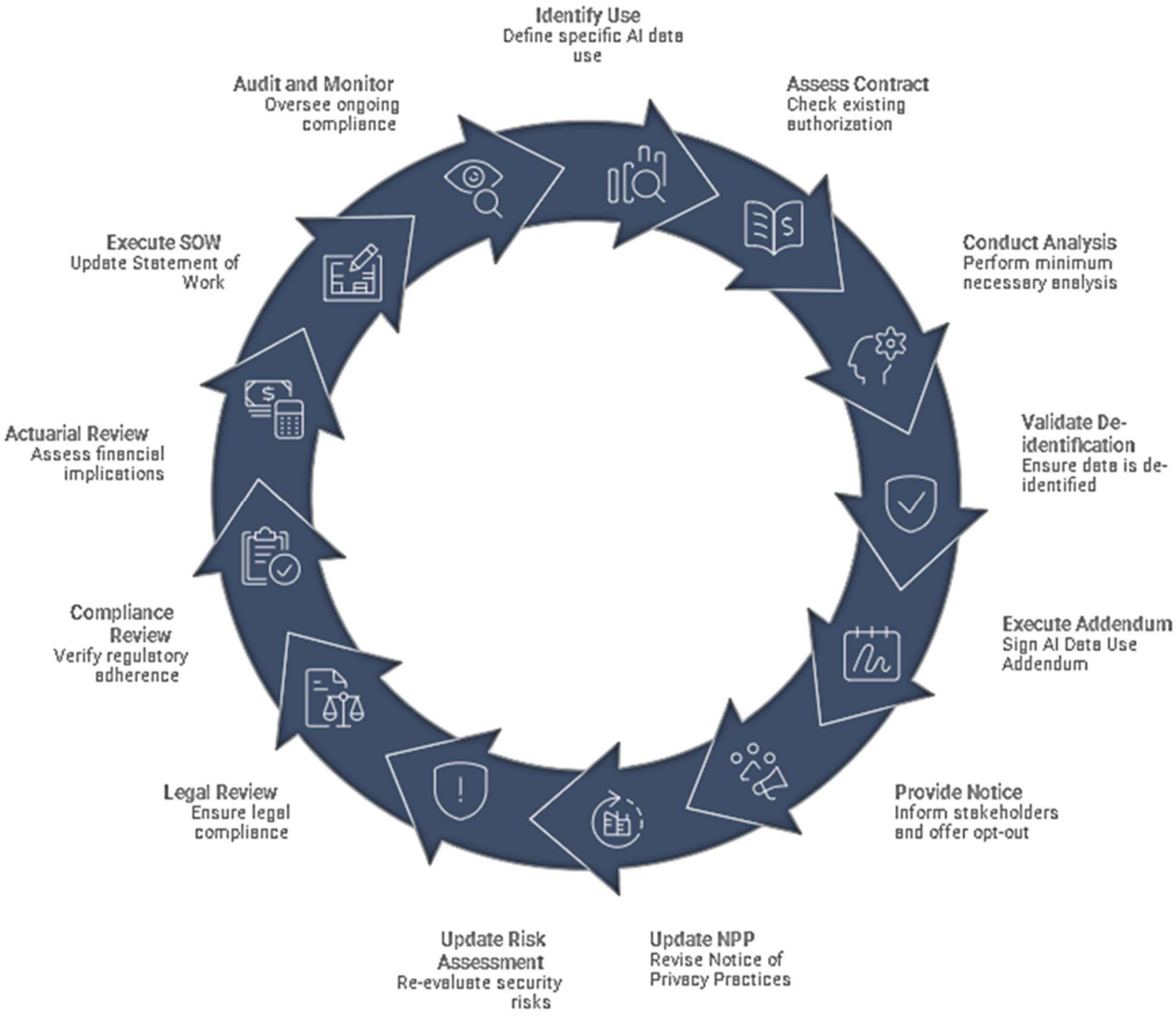
Introduction of AI data uses triggers the HIPAA Notice of Privacy Practices material change requirement under 45 CFR § 164.520. Updated NPPs must be actively redistributed to existing members and clients — not merely posted on a website.

Notice Element	Standard Language	AI-Aware Required Addition
Data use description	TPO categories, marketing opt-outs	AI processing purposes, model training, automated inference, decision support
Vendor disclosure	BA relationships generally described	AI vendors, model operators, AI sub-processors enumerated or categorically described
Individual rights	Access, amendment, accounting	Right to opt out of AI-driven decision support; applicable state law AI rights
Security practices	Safeguard categories described generally	AI-specific controls; model access restrictions; inference attack mitigations
Material change trigger	New uses, new disclosures	+ Introduction of AI; change of AI vendor; model retraining events

PART 8 GOVERNANCE CHECKLIST: AI DATA USE AUTHORIZATION SEQUENCE

8.1 Pre-Engagement Authorization Sequence

The following sequence must be completed before any AI use of healthcare data begins. This is not a compliance formality — it is the mechanism that protects initiative investments and enables POCs to move to production.



#	Required Action	Responsible Party	Instruments
1	Identify and document the proposed AI use: data set, purpose, model type, retention, output disposition	Vendor / Plan	SOW draft
2	Assess whether existing MSA, BAA, DUA, SOW authorize the proposed use — default presumption is they do not	Legal / Compliance	All instruments
3	Conduct minimum necessary analysis: what data, what granularity, what time window, and why — documented	Privacy Officer	BAA / DUA
4	De-identification validation. Expert Determination; prior certifications do not extend to new AI processing	Qualified Statistician	DUA
5	Draft and execute AI Data Use Addendum to MSA, BAA, DUA before any data is accessed	Legal	MSA + BAA + DUA
6	Provide written notice to covered entity client:use, data, model, retention; meaningful opt-out window	Vendor	Client notification
7	Update HIPAA NPP for material change; actively redistribute to members — not merely post	Privacy Officer	NPP

#	Required Action	Responsible Party	Instruments
8	Update security risk assessment for new processing modality; document AI-specific threat vectors	Security Officer	Risk assessment
9	Legal review: HIPAA, CMS, state AI laws, applicable accreditation standards	Legal	All
10	Compliance review: minimum necessary, FDR flow-down (if MA), access controls, audit logging	Compliance	All
11	Actuarial review when AI affects UM, risk strat, benefit determination, pricing assumptions	Actuary	SOW / reg filings
12	Execute updated SOW: AI-specific scope, restrictions, IP ownership, termination provisions	Legal / Contract	SOW
13	Establish ongoing audit/monitoring for AI use compliance. Model retraining events restart sequence.	Compliance / Privacy	Ongoing

!Retroactive Amendment Note A retroactive BAA or MSA amendment does not cure a prior unauthorized data use. If PHI was used beyond authorized scope, the violation occurred at the time of use. Retroactive amendments may limit future exposure but do not eliminate past compliance risk. The enforcement record does not support treating retroactive ratification as a cure.

MA FDR-Specific Note
For Medicare Advantage plans and their FDR chains: all AI data use authorization requirements apply in addition to, not instead of, the mandatory FDR provisions in Part 6. An AI vendor that is an FDR must satisfy both sets of requirements. The plan remains federally accountable for compliance regardless of contractual delegation.