OlenArc

FIELD GUIDE

TRIBAL HEALTH · PROCUREMENT

Tribal Data Sovereignty Vendor Readiness Guide

Practical questions for Tribal health organizations choosing AI, data, and technology vendors.

Compiled by OlenArc · July 7, 2026 · Meeting & procurement guide · Not legal advice · Not a sales document

Made to bring into the room — for Tribal health leaders, Native-serving health centers, Tribal clinics and Indian health programs, Tribal Epidemiology Centers, health boards, procurement teams, and program directors.

A note on neutrality. OlenArc builds software, so we're a vendor too. This guide is **not a sales document** and recommends no vendor — including us; we'd genuinely encourage you to ask us the same questions. We simply compiled existing public frameworks (Indigenous data governance, CARE, HHS, ONC, HIPAA, NIST) into plain-language questions. It is decision-support, **not legal advice** — customize it with your Tribal Nation's laws, policies, governance, and legal counsel.

01 — THE CORE MESSAGE

The real question isn't whether the tool works

Many vendors now say they use "AI," "data," "analytics," or "automation." For a Tribal health organization, the bigger question is simple:

Will this vendor respect Tribal authority over data about our people, our patients, our programs, and our communities?

Tribal data sovereignty is the right of Native Nations to govern how data about their people, lands, services, and communities is collected, stored, used, shared, interpreted, and returned. It is not only a privacy issue — it is a governance, trust, and sovereignty issue.

Health data can affect funding, services, clinical decisions, public health planning, grants, eligibility, research, and how outside systems describe the community. A vendor should not be able to turn Tribal data into a product, dataset, AI model, or business advantage unless the Tribal organization clearly understands it and approves it.

HIPAA is necessary — but HIPAA is not enough.

HIPAA focuses mainly on individual protected health information. Tribal data sovereignty also covers collective rights, Tribal governance, access, interpretation, secondary use, de-identified data, AI training, community-level harm, benefit sharing, data return, and long-term capacity.

02 — THE SIMPLE STANDARD

Six promises a good vendor should make in writing

PROMISE 1

Your data stays yours

The vendor is a service provider, not the owner. "Tribal data" includes patient, program, community, and public-health data, plus reports, metadata, logs, and AI outputs.

PROMISE 2

You can access & export your data

Get your data back in usable formats — raw data, reports, attachments, logs, metadata — for care, reporting, grants, audit, or moving to another system. No lock-in.

PROMISE 3

No secondary use without written approval

No AI training, product development, benchmarking, research, resale, or "de-identified / aggregated" datasets without clear written Tribal approval. De-identification is not the same as approval.

PROMISE 4

AI must be explainable enough to review

If AI, risk scoring, or automated decisions are used, the vendor explains what it does, what data it uses, its limits, whether humans review it, and how mistakes are fixed.

PROMISE 5

You can leave without losing control

At contract end: data returned, migration supported, copies deleted where appropriate, and deletion certified — including backups, subcontractor copies, and AI artifacts.

PROMISE 6

The work benefits the Tribe

Not only the vendor. Staff training, documentation, data dictionaries, admin access, and knowledge transfer that build long-term Tribal capacity (the CARE "Collective Benefit").

03 — THE FRAMEWORKS, IN PLAIN ENGLISH

Where this guide comes from

The goal is not to make procurement complicated. It is to turn strong, existing principles into simple vendor questions.

Indigenous Data Sovereignty	Native Nations have the right to govern data about themselves — how it is collected, owned, used, shared, interpreted, and applied.
CARE Principles	**C**ollective Benefit · **A**uthority to Control · **R**esponsibility · **E**thics. Data work should benefit Indigenous communities, stay under their authority, and reduce harm.
CARE Data Maturity Model	Moves CARE from principles into actual practices — a way to ask whether a vendor only uses good language or actually has policies and systems behind it.
OCAP®	Ownership, Control, Access, Possession — a First Nations framework from Canada (**not U.S. law**), useful language for making "who owns / controls / can access / holds the data" concrete.
HHS Tribal & TEC Data Access	Department-wide policies giving Tribes and Tribal Epidemiology Centers access to data to serve their communities — access, not just privacy that keeps data locked away.
HIPAA & BAAs	Important, but the floor. A Business Associate Agreement limits how a vendor uses PHI and requires safeguards — it does not answer AI training, secondary use, collective benefit, or Tribal governance.
AI transparency	ONC's HTI-1 sets transparency expectations for predictive decision support in certified health IT; HHS Section 1557 applies nondiscrimination to patient-care decision-support tools; NIST's AI Risk Management Framework structures govern / map / measure / manage.

04 — ASK BEFORE SIGNING

Vendor questions, grouped for the meeting

A · DATA OWNERSHIP & CONTROL

- [ ] Under your standard contract, who owns the data in the system?
- [ ] Will you recognize in writing that our organization controls our data?
- [ ] How do you define "Tribal data" — does it include program, public-health, community data, reports, logs, metadata, and AI outputs?
- [ ] Can our governance body, health board, or data steward approve or deny new data uses?

B · ACCESS, EXPORT & PORTABILITY

- [ ] Can we export all of our data at any time, and in what formats?
- [ ] Does export include raw data, reports, attachments, audit logs, and metadata?
- [ ] Is there a fee for export or migration, and how fast can you deliver a full export?
- [ ] Can our staff access the data directly without always needing vendor support?

C · SECONDARY USE & AI TRAINING

- [ ] Do you use customer data to train AI models?
- [ ] Do you use it for product improvement, benchmarking, research, analytics, or resale?
- [ ] Do you use de-identified or aggregated data for anything outside our direct services?
- [ ] Can we opt out of all secondary use — and will you put "no AI training or secondary use without written Tribal approval" in the contract?

D · HIPAA, SECURITY & SUBCONTRACTORS

- [ ] Will you sign a HIPAA Business Associate Agreement if PHI is involved?
- [ ] Where is the data stored, and which cloud providers or subcontractors touch it?
- [ ] Will you disclose all subcontractors and bind them to the same obligations?
- [ ] Do you use encryption, role-based access, audit logs, and backups — and how fast will you notify us of a breach?

E · AI TRANSPARENCY, BIAS & HUMAN REVIEW

- [ ] Does your product use AI, machine learning, predictive analytics, or automated decision support?
- [ ] What data was it trained on, and was it tested with American Indian / Alaska Native populations?
- [ ] What are the known limitations — and can our staff override the AI or turn it off?
- [ ] How do you monitor errors, bias, and harm after deployment? Do you provide model cards or plain-language AI documentation?

F · EXIT, DELETION & RETENTION

- [ ] What happens to our data when the contract ends?
- [ ] Will you return all data in usable formats and delete copies no longer needed?
- [ ] Will you certify deletion — including backups and subcontractor copies?
- [ ] What happens to AI artifacts, embeddings, analytics outputs, or derived datasets made from our data?

G · TRIBAL BENEFIT & CAPACITY BUILDING

- [ ] How will your work strengthen our organization's internal capacity?

- [ ] Will you train our staff and provide documentation and data dictionaries?
- [ ] Can we maintain or transition the system without depending on you forever?
- [ ] If our data helps improve your product, how does our community benefit?

05 — WORTH A SECOND LOOK

Answers worth one more question

None of these are automatic deal-breakers.

A good vendor — large or small — can usually work through them. They're just the answers worth slowing down on and asking one more question before you sign. The goal is a clear conversation, not a disqualification.

“We own all data in our platform.”

Ask next — can we add language that says our organization controls the data and can export it any time?

“HIPAA compliance covers this.”

Ask next — HIPAA covers individual PHI; how do you handle ownership, secondary use, and our governance on top of it?

“We can use de-identified data however we want.”

Ask next — for what purpose? Even de-identified data can affect communities, so it's worth naming the uses in writing.

“Our AI is proprietary, so we can't share details.”

Ask next — fair to protect your IP — can you still explain intended use, limits, and how our staff can review or override it?

“You can export reports, but not the raw data.”

Ask next — can we also export the underlying data, logs, and files, so we're not locked in if we ever move?

“Subcontractors are confidential.”

Ask next — can we get the list of who touches our data — cloud, analytics, AI, support — bound by the same terms?

“We use customer data to improve our models by default.”

Ask next — can we opt out, or set it so training on our data needs our written approval first?

“Deletion is not possible.”

Ask next — some retention is normal — can you walk us through retention, deletion, backups, and certification so it's clear?

“Everyone gets the same contract.”

Ask next — would you adjust a few terms for a Tribal organization? Many vendors will once it's asked.

06 — RAISE WITH COUNSEL

Contract topics to discuss

Not legal advice — a list of topics to raise with legal counsel or procurement staff.

01

Definition of Tribal Data

Broad enough to include members, patients, programs, public health, community services, governance, reports, metadata, logs, and AI outputs.

02

Tribal control & approval

Data used only for approved purposes; any new use needs written approval from the Tribal organization or designated authority.

03

No AI training without approval

Clearly prohibit AI training, fine-tuning, benchmarking, and commercial analytics on Tribal data absent written approval.

04

Access & export

Guarantee timely export in usable formats — raw data, reports, attachments, metadata, audit logs, documentation.

05

Subcontractors & flow-down

Disclose subcontractors; require them to follow the same privacy, security, sovereignty, and deletion obligations.

06

HIPAA & BAA

If PHI is involved, a signed BAA that matches the actual services, cloud providers, subcontractors, and data flows.

07

AI transparency & monitoring

Plain-language documentation, intended-use limits, human review, bias monitoring, and the ability to suspend or turn off AI.

08

Incident notice

Define how fast the vendor must report breaches, unauthorized access, or harmful AI behavior.

09

Exit, return, deletion, certification

What happens at the end: return, migration, deletion, backups, subcontractor copies, and certification.

10

Benefit & capacity building

Staff training, documentation, reporting support, data dictionaries, knowledge transfer.

07 — SAY IT OUT LOUD

A simple meeting script

OPEN THE CONVERSATION

“Before we talk about features, we need to understand your approach to Tribal data sovereignty. Our data connects to our patients, community, programs, funding, and governance. We need to know how you handle ownership, access, secondary use, AI training, subcontractors, export, deletion, and Tribal approval before we can move forward.”

THEN ASK

“Can you show us, in writing, where your contract says we control our data and you cannot use it for secondary purposes or AI training without written approval?”

AND

“If we end the contract, how do we get all of our data back, and what proof do we receive that remaining copies were deleted where appropriate?”

IF AI IS INVOLVED

“Can you explain what the AI does, what data it was trained on, what it should not be used for, how humans review it, and how you monitor bias or harm for Native communities?”

08 — DURING PROCUREMENT

The practical vendor scorecard

AREA	GREEN FLAG	YELLOW FLAG	RED FLAG
Data ownership	Contract clearly says the Tribal organization controls data	Says "customer data" but is vague	Vendor claims ownership or broad usage rights
Data access	Full export, usable formats, logs & metadata included	Reports export only	Raw data unavailable or expensive
Secondary use	No reuse without written approval	Opt-out possible but unclear	Uses de-identified / aggregated data by default
AI training	No AI training without written approval	AI terms unclear	Customer data trains models by default
HIPAA	BAA available if PHI is involved	Says "HIPAA-aware" but no BAA	Refuses BAA while handling PHI
Subcontractors	Disclosed and bound by same terms	Partial list only	Refuses to disclose
AI transparency	Plain-language docs and human override	Some docs, limited subgroup testing	"Proprietary, cannot explain"
Bias monitoring	Ongoing review and incident process	General fairness language	No monitoring or no answer
Exit	Clear return, migration, deletion, certification	Export available but limited	Lock-in, high fees, no deletion clarity
Tribal governance	Approval workflow recognized	Informal approval only	Vendor ignores Tribal governance

10 Questions Before Signing

Tear sheet — bring this one page to any AI, healthcare, data, or software vendor meeting.

1. **Who owns and controls our data?**
2. **Can we export all of our data** — including raw data, files, logs, and metadata?
3. **Will you agree not to use our data for AI training or secondary use** without written approval?
4. **Do you use de-identified or aggregated customer data?** If yes, for what purpose?
5. **Will you sign a HIPAA BAA** if PHI is involved?
6. **Which subcontractors, cloud providers, or AI services** will touch our data?
7. **If AI is used, can you explain** what it does, what data it uses, and its limitations?
8. **How do you test for bias or harm,** especially for American Indian / Alaska Native populations?
9. **Can we turn off, override, or review AI outputs** before they affect care or services?
10. **If we leave, how do we get our data back,** and how do you prove deletion where appropriate?

> **Best short rule:** If a vendor cannot explain ownership, access, reuse, AI training, subcontractors, export, and deletion in plain language, they are not ready for a Tribal health data relationship.

› RECOMMENDED NEXT STEPS

Putting it to work

① Add these questions to every vendor demo and RFP. ② Require answers **in writing**, not only verbally. ③ Have counsel review ownership, secondary use, AI training, and deletion terms.

④ Keep a list of approved and prohibited data uses. ⑤ Name who can approve new uses — Council, health board, CEO, data-governance committee, TEC, or a data steward. ⑥ Require export & exit terms **before** launch.

⑦ For AI tools, require human review, plain-language documentation, and the ability to turn off risky features.

⑧ Revisit vendor terms annually — AI products change quickly, and yesterday's answers may no longer hold.

A note on who compiled this

OlenArc is a small software studio that builds tools for Native-serving programs — which makes us a vendor too. We pulled this together from public Indigenous data-governance, HHS, ONC, and NIST frameworks; it recommends no vendor, including us, and we'd genuinely encourage you to hold us to the same questions. For what it's worth, our own standard is simple: **the client owns and can export its data, there's no lock-in, we don't resell it, and we don't train models on it.**

§ SOURCE NOTES

What this guide is built from

Indigenous data governance: Native Nations Institute (Indigenous Data Sovereignty & Governance) · Global Indigenous Data Alliance & the CARE Principles · CARE Data Maturity Model · US Indigenous Data Sovereignty Network · Collaboratory for Indigenous Data Governance · First Nations OCAP® (a Canadian First Nations framework, not U.S. law). **Federal health & privacy:** HHS Tribal Data Access and TEC data-access policies · HHS HIPAA guidance on Business Associate Agreements, de-identification (Safe Harbor / Expert Determination), and cloud computing. **AI governance:** ONC HTI-1 transparency expectations for predictive decision support · HHS Section 1557 nondiscrimination guidance for patient-care decision-support tools · NIST AI Risk Management Framework · American Indian Health Commission of Washington — Tribal Data Sovereignty & Data Privacy resources.

Note: This guide should be customized to each Tribal Nation's laws, policies, governance structure, and legal counsel. It is decision-support, not legal advice, and makes no compliance certification. Legal obligations (including under Section 1557) may change; verify current requirements with counsel.