Secure Nomad

Enterprise security, practice-sized.

FREE ARTIFACT 3 OF 3 · THE APPROVE / REMEDIATE / REJECT DECISION TREE

Approve · Remediate · Reject

The AI vendor decision tree · three gates, in order · one page

An AI feature that touches PHI

↓

GATE 1 · BAA ADEQUACY

Does the contract cover today's data flows, name the subprocessors, and address training use?

Evidence: the BAA adequacy template, the vendor's written answers to questions 5 to 8, amendment status.

→ **REJECT**
No coverage and no path to amendment. Full stop. When PHI trains their models with no opt-out, subprocessors are undisclosed, and they will not answer in writing, the answer is reject. The written no is itself file evidence.

↓ PASS, OR PASS ON A PENDING AMENDMENT

GATE 2 · DATA MINIMIZATION

Can the integration be configured to send only what the feature needs?

Evidence: the two-column field map (needs vs sends), configuration screenshots from your own console. A settings panel is evidence. A sales deck is not.

→ **REMEDIATE**
Configurable gap. Restrict scope, redact or de-identify before transmission, set a deadline and an owner, document the configuration.

→ **REJECT or REMEDIATE with vendor commitment**
Not restrictable and over-sends PHI. Reject when the over-send is full-room audio, third parties, or training data.

↓ ALREADY CONFIGURED, OR REMEDIATION SCHEDULED

GATE 3 · OPERATIONAL OWNERSHIP

Does a named person own monitoring this feature?

Evidence: the vendor's release notes subscribed from your mailbox, a quarterly hour on the calendar, a name next to it.

→ **APPROVE**
Dated, with the written basis. Every approve, remediate, or reject decision goes in the file with its reasons.

→ **NOT APPROVED**
If nobody owns it, it is not approved. It is abandoned in production. Name an owner, then re-run Gate 3.

Worked example: the ambient scribe.

Enabled by a physician from the EHR marketplace; IT had never heard of it. **Gate 1:** coverage was the EHR's 2023 master agreement, silent on audio capture and the scribe's model subprocessor. Amendment demanded, vendor willing. **Gate 2:** full-room audio crossed the boundary, family and staff included. Provider-only capture was configurable. **Gate 3:** nobody owned the release notes; a summarization model had shipped mid-year unnoticed. Owner named. **Verdict: remediate, sixty days, documented.**

Three rules

- **Gates in order.** Do not weigh a great feature against a silent contract.
- **A written no is a valid outcome.** Rejecting on evidence proves diligence.
- **"Approved" without an owner is "abandoned in production."** Gate 3 is not optional.

Record per feature: gate results, the decision, a written basis of two to five sentences citing the evidence, and for remediate, the actions with owners and dates.

Ricky Martin
CISSP, CCSP, CISM · twenty years in enterprise cybersecurity, now working only with independent practices.

securenomad.ai/ISACA
ISACA New England 50th AGM · September 10, 2026

Free to use and share. No forms, no gate. Not legal advice.