Palo Alto Health Labs

A PHI Data-Flow Mapping Template

Not legal advice. Not a compliance certification.

Purpose: document where information could travel during one defined workflow. Use system labels, not actual patient information. The mapping exercise does not itself determine whether HIPAA applies or authorize a disclosure.

Project/version: _____ Workflow: _____
Map owner: _____ Reviewed on: _____
Intended user and task: _____
Starting event: _____ Final outcome: _____
Legal-role/scope reviewer and evidence reference: _____

1. Draw the path

Place one box per actual system boundary. Include only components present, then add overlooked destinations. Label each arrow using the transfer register below.

Illustrative path, not an approved architecture:

User/browser → Upload endpoint → Application runtime → Database/storage
↓
Model/API intermediary → Model provider

Side paths to check: error tracking; analytics; notifications; support; backups; exports; local cache; coding/debugging tools. An optional component is still a review question, not presumed permission to send PHI.

2. System register

System ID/name	Legal vendor / exact product	Account/project + plan/add-on	Purpose	Data classes, no examples	Owner
A					
B					
C					
D					

For each system separately record:

- Hosting/processing region evidence: _____
- Storage/caches/backups and retention/deletion evidence: _____
- Access roles and privileged administrators: _____
- Required agreement / signed scope evidence / reviewer: _____
- Model/feature/connector exclusions: _____
- Configuration evidence and last review date: _____
- Status: Confirmed by accountable reviewer / Open / Not applicable with reason.

3. Transfer register — one row per arrow

Transfer ID	From → to	Trigger / purpose	Data classes	Read / write / export	Access/auth mechanism	Log/cache destinations	Reviewer / open issue
T1							
T2							
T3							

Record whether each transfer is necessary for the defined task and what narrower payload could work. Document encryption/configuration evidence using references; do not paste keys or tokens.

4. Walk through a single synthetic transaction

- Can you identify every recipient of input and output? _____
- What survives a browser refresh or user logout? _____
- What is copied on an error or support request? _____
- Do model requests pass through another vendor? _____
- What appears in URLs, logs, traces, exports and backup copies? _____
- Who can read/restore/delete each copy? _____
- What happens after cancellation, failure or account closure? _____

HL7 warns that HTTP logs, even URLs, can disclose sensitive information. HHS explains that encrypted ePHI storage can still create a business-associate relationship even if the provider lacks the key.

5. Resolve the boundary

Open boundary	Question / evidence needed	Interim restriction	Owner / due	Resolution / date

Proposed interim rule: do not introduce real patient data into an unresolved processing path. Do not treat a vendor logo or available BAA as evidence of executed, service-specific coverage. A BAA is not sufficient alone; HHS also requires other applicable safeguards and risk analysis.

Review participants: _____
Next review trigger (new vendor/feature/export/intended use): _____
Decision/evidence reference: _____

Sources

- HHS cloud guidance <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, opened/read 2026-11-07 PST.
- HL7 FHIR R4 security <https://hl7.org/fhir/R4/security.html>, opened/read 2026-11-07 PST.

Limits

Checkboxes and decision gates are proposed practices, not a complete legal checklist, clinical validation instrument or compliance certification.

No PAHL delivery capability or client outcome is asserted.

Do not enter patient identifiers, PHI, credentials or access tokens in these worksheets; use system labels and approved evidence references instead.

Not legal advice.

Do not invent a booking URL, availability or deliverables for the free call.