

Client Data Privacy Checklist

Program leaders, privacy/IT owners, and staff handling sensitive records

Before client information meets AI

For planning and internal review. This checklist does not authorize a data disclosure.

Default for beginner exercises

Use public or fully fictional information. Do not upload client records, case notes, health details, identifiable stories, or private contact information as part of a starter exercise.

1 / Define the purpose

- ☐ The task and intended benefit are specific.
- ☐ The use needs the proposed data.
- ☐ A less sensitive or non-AI alternative was considered.
- ☐ A responsible program owner can explain the decision.

2 / Inventory the data

- ☐ Required fields and sources are listed.
- ☐ Direct identifiers and identifying combinations are understood.
- ☐ Files, images, comments, and metadata were considered.
- ☐ Unnecessary fields are excluded.

3 / Confirm authority

- ☐ The designated privacy/IT reviewer assessed this use.
- ☐ Organizational permissions and applicable obligations were reviewed.
- ☐ Any needed agreements or permissions are in place.
- ☐ Approval covers the exact account, tool, data, and purpose.

Client Data Privacy Checklist

Review the full data path

Client information can pass through more than the AI screen.

4 / Vendor and account review

- ☐ The precise account/plan/environment is recorded.
- ☐ Data use for training or improvement was reviewed.
- ☐ Retention, deletion, and support access were reviewed.
- ☐ Connected apps and subprocessors were considered.
- ☐ Required agreements and settings were verified by the owner.

5 / Access and storage

- ☐ Only authorized people can access inputs and outputs.
- ☐ Sharing defaults and public-link behavior are understood.
- ☐ Export locations and run logs are part of the assessment.
- ☐ Secrets remain outside prompts and documents.
- ☐ Records follow the organization's retention requirements.

6 / Output and people

- ☐ A qualified person checks facts and meaning.
- ☐ Generated output cannot make consequential decisions alone.
- ☐ Reidentification risks in summaries or small groups were reviewed.
- ☐ The team considered dignity, context, and potential bias.

Important distinction

A plan name, a vendor claim, consent, or deleting names does not by itself resolve all obligations. Route uncertainty to the designated reviewer instead of treating this checklist as permission.

Client Data Privacy Checklist

Decision and incident readiness

Complete this record before any approved use begins.

7 / Operational readiness

- ☐ Staff know the approved boundaries.
- ☐ A reporting contact and backup are named.
- ☐ The team knows how to pause the workflow.
- ☐ A response owner will direct containment and follow-up.
- ☐ Tool or data changes trigger another review.

Approval record

Use case: _____

Exact tool/account: _____

Permitted fields and sources: _____

Excluded information: _____

Controls and approval evidence: _____

Owner, reviewer, and date: _____

Review/expiry date: _____

Decision: ☐ Approved within documented scope ☐ Hold

If something is entered by mistake

Stop entering more information. Promptly notify the designated contact through the organization's reporting process. Preserve the facts requested by the response owner, including tool/account, time, data category, and actions already taken. Follow their directions. Do not paste the sensitive material into another tool to investigate.

Reporting details

Primary contact/channel: _____

Backup contact: _____

Manual fallback: _____

Client Data Privacy Checklist

Practice a safer alternative

Fictional scenario for a team discussion.

Scenario

A program manager wants a case-note summary for staff handoff. The proposed tool is a personal AI account. No one can confirm the approved data types or vendor terms.

A responsible next step

Hold the upload. Ask the designated privacy/IT reviewer to assess the exact use and account. Use a completely fictional note to explore what a useful summary format might look like. A fictional practice exercise does not authorize uploading a real note later.

Discussion questions

What minimum information would the actual task require? Who has authority to approve the use? Where would input, output, and logs live? Who checks the summary? What happens if the system invents an event or omits an important fact?

Further reading

NIST AI Risk Management Framework:

<https://www.nist.gov/itl/ai-risk-management-framework>

For general risk-management context. This checklist is a practical HLTF planning tool, not a certification or a complete legal/privacy assessment.