Worked four-factor assessment

Healthcare incident responders and privacy officers

Read the complete guide on aona.ai

An impermissible PHI disclosure is presumed to be a breach unless the required assessment demonstrates a low probability of compromise or an applicable exception applies. After an AI submission, preserve the facts, assess the recipient and exposure, and involve the privacy and incident owners promptly.

A fictional employee submits two identifiable patient summaries to an unapproved AI account. The assessment identifies evidence needs without inventing a final legal conclusion.

Synthetic incident only. No real patients, provider response, notice or completed investigation is represented.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Secure the factual record**

Capture the exact service, account, time, data categories and source evidence without copying PHI unnecessarily.

☐ **Address each HHS factor**

Separate established facts from unknown acquisition, recipient and mitigation details.

☐ **Assign the legal decision**

Record the responsible privacy owner, the unsecured-PHI assessment and applicable notification steps and dates; this worksheet does not send notices.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Factor	Invented case fact	Assessment and next step
Nature and extent	Two invented records include names and diagnoses.	Direct identifiers and health details require careful assessment; verify the actual payload.

Factor	Invented case fact	Assessment and next step
Unauthorised recipient	An external AI account was used; its applicable terms are not established.	Identify the service, account and any other recipients before assessing their obligations.
Acquired or viewed	Employee saw an answer; provider access and retention facts are unknown.	Do not infer no acquisition from the absence of a human viewer; obtain relevant evidence.
Mitigation	A deletion request is proposed but not sent in this exercise.	Record any actual action and response; do not treat a draft request as completed mitigation.
Illustrative disposition	Material recipient and exposure facts remain unresolved.	No low-probability conclusion is demonstrated by this example; escalate the assessment.

Four questions before a conclusion

- **Data:** What PHI and identifiers were involved?
- **Recipient:** Who received or could access it?
- **Exposure:** Was it acquired or viewed?
- **Mitigation:** What was actually done and evidenced?

Synthetic evidence request list

- What exact information was submitted, through which account and feature?
- Was the PHI unsecured under the applicable guidance, and what evidence supports that assessment?
- Was the input stopped locally or received by the service?
- Which entity and other recipients could process or access it?
- What retention, access and deletion facts can the provider substantiate?
- What mitigation was actually completed, and when?

Example decision record

Assessment status: facts incomplete.
Low-probability conclusion: not demonstrated by this fictional evidence.
Notification determination: for the authorised privacy/legal owner.
Notices sent: none; this is a teaching exercise.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information; no professional approval or installed-product result is represented. Aona does not determine reportability, erase third-party copies or submit HIPAA breach notifications.

HHS: Breach Notification Rule. The presumption of breach, four risk factors, exceptions and notification responsibilities and time limits.

HHS: Guidance on HIPAA and cloud computing. Business-associate roles, BAAs, risk analysis and cloud-service safeguards, including providers without decryption keys.

45 CFR 164.404 and the unsecured PHI condition. Individual notification after discovery of a breach of unsecured PHI, without unreasonable delay and within the applicable outer time limit; unsecured PHI is defined in 45 CFR 164.402.