



EVIDENCE & RESOLUTION

Claim Document Sharing and Privacy Workbook

Verify the requester, understand the request, organize authorized disclosure and retain a clear record of what was shared.

WHAT THIS WORKBOOK HELPS YOU DO

01

Complete your request and identity verification

02

Complete your authorization scope review

03

Complete your disclosure set and delivery ledger

A claimant receiving requests for identification, medical records, authorizations, account information or large document uploads.

Use it on screen or on paper. Save a personal copy before entering information. Blank response areas are fillable; printed copies work just as well. Keep completed copies private.

Scope. Educational organization tools, not legal, medical, tax or financial advice. No claim result, coverage decision or payment is promised. Verify policy language, current local rules and all deadlines with the appropriate professional or official source.



START HERE

Start with a clear working file

Work on one claim, account or issue at a time. Keep originals unchanged and label working copies with a short evidence ID. Complete the guidance in order, then use the worksheets to turn questions into an organized next step.

A practical order

- 01 Read the four guidance pages before filling the worksheets. Mark facts you can support and questions that still need an answer.

GUIDANCE / PAGES 03-06

- 02 Use the fictional examples to check your method. Their facts and dollar amounts do not describe your claim or predict an outcome.

EXAMPLES / PAGE 07

- 03 Complete the four working sheets, then use the readiness check and next-step page. Duplicate a worksheet when you need another record.

WORKSHEETS / PAGES 08-11

Protect your information

Store completed copies somewhere private. Use a claim or account suffix when a full identifier is unnecessary. Share only relevant copies through a verified recipient and appropriate channel. A saved PDF can contain personal information even when it is not open on screen.

Before a deadline. Do not wait to finish this workbook when a notice, release, court paper or policy deadline needs attention. Verify the actual requirement and seek qualified help promptly.



GUIDANCE 1

01

Capture the request before responding

Save the message, letter or form and record who appears to be asking, what is requested, the stated purpose, the proposed deadline and the delivery method. Do not assume that a familiar logo or a reference to your accident proves the sender's identity. A rushed phone call can leave important questions unanswered. Ask for the request in writing when practical, and separate a routine document request from a demand for credentials, account access or a signed authorization. Keep the original message so you can verify exactly what was said.

Verify the person through an independent route

Use a phone number, official portal or contact you already know is genuine to confirm an unexpected request. Do not rely only on a number or link inside the suspicious message. Verify the organization, staff member, case reference and intended recipient. If there is a mismatch, pause transmission while you ask the legitimate organization what is happening. Avoid sending passwords, one-time security codes or unrestricted account access as a way to prove identity. This verification step reduces avoidable disclosure; it does not determine whether the substantive request is legally valid.

RELATED WORKING SHEETS

- Request and identity verification
- Authorization scope review

Sources for this page: [1], [2], [3], [4]. See the linked source guide.



GUIDANCE 2

Understand scope and authority 02

Read what the form actually permits: who may disclose, who may receive, what information, which dates, the purpose and the expiration or ending event. A medical authorization is different from a request for a copy of your own records or a routine treatment consent. Highlight language you do not understand and ask the relevant provider, insurer or counsel to explain it. Do not assume that broad wording is always improper, or that changing a form yourself will be accepted. Your aim is an informed decision based on the request and your obligations.

Create a working disclosure set

Keep an unchanged source copy and assemble only the set you are authorized or required to provide. Use clear filenames and an index so the recipient can tell what is included and what remains outstanding. If a document concerns another person, contains unrelated sensitive information or combines several accounts, ask how it should be handled before sharing. Redaction may require care and may be inappropriate for a particular legal request; a black rectangle on a PDF does not necessarily remove hidden text. Do not alter evidence to hide relevant information.

RELATED WORKING SHEETS

- Authorization scope review
- Disclosure set and delivery ledger

Sources for this page: [1], [2], [3], [4]. See the linked source guide.



GUIDANCE 3

03

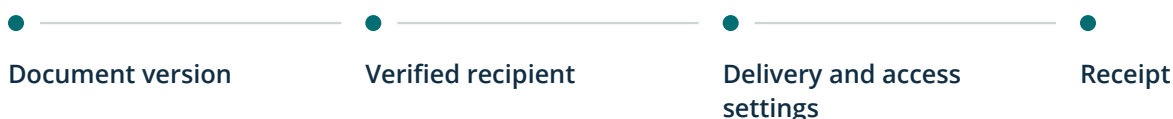
Choose the verified delivery method

Confirm the official portal, email address or mailing destination and the requested file format. A convenience link sent by an unknown party is not a reason to upload a whole claim archive. Check that the sharing setting gives access only to the intended recipients and avoid public links. Do not store passwords or full identity numbers in the tracking worksheet. If the organization requires a sensitive identifier, ask about its secure process and use that process directly rather than putting it in an ordinary message.

Keep a disclosure and authorization record

Record the exact document versions, recipient, date, purpose and confirmation of receipt. Keep a copy of signed authorizations and any later changes, with their effective scope. An authorization's expiration does not necessarily undo disclosures already made. Likewise, revocation can have limits and procedural requirements. If you are considering revoking permission, consult the actual form, the covered entity's process and appropriate advice about effects on the claim. Do not confuse asking for a restriction with obtaining an agreed restriction.

Connect each shared version with the verified destination, access setting, and delivery record.



Sources for this page: [1], [2], [3], [4]. See the linked source guide.



GUIDANCE 4

04

Respond to a suspected mistake or scam

If material may have gone to the wrong recipient or a request appears fraudulent, preserve the messages and contact the legitimate organization through a verified route. Record what information was exposed and when, without spreading it further. Use official recovery resources where identity theft or account compromise is suspected. Do not pay a stranger who promises to erase information or release settlement money after a fee. Seek legal or professional help if the event affects confidential records, court obligations or another person's information.

Close access carefully without destroying records

When a delivery is complete, review whether a temporary sharing link should expire or access should be removed under the agreed process. Keep the underlying records and the disclosure history for applicable legal and practical needs. Do not delete relevant evidence simply to improve privacy or follow a generic cleanup checklist while a claim or legal hold remains active. Privacy and preservation need to be managed together. Finish with a summary of active permissions, outstanding requests and questions that require counsel or the organization's privacy office.

RELATED WORKING SHEETS

- Access and incident review
- Disclosure set and delivery ledger

Sources for this page: [1], [2], [3], [4]. See the linked source guide.



FICTIONAL EXAMPLES

Work through the examples

These invented cases demonstrate the method. They are not case results, estimates of what you will receive or statements of universal rights.

01 A genuine company, unverified message

A message uses the insurer's name and asks for a document upload.

Next step: Verify the request through an existing official contact and use the confirmed secure destination.

Avoid. Treating branding alone as verification.

02 A request for every record

An authorization is broader than the claimant expected.

Next step: Clarify purpose, scope and obligations with the requester and counsel before deciding.

Avoid. Assuming either automatic refusal or automatic signature is always correct.



WORKSHEET 1

01

Request and identity verification

Confirm unexpected requests through an independent known contact.

Request date/source

Organization/person

Data sought

Stated purpose/deadline

Independent verification route

Identity confirmed

Unresolved concern

[Related guidance: Capture the request before responding](#)



WORKSHEET 2

02

Authorization scope review

This is an analysis sheet, not a valid authorization.

Discloser

Recipient

Information/date range

Purpose

Expiration/event

Revocation instructions

Claim obligation question

Professional answer

Related guidance: [Understand scope and authority](#)



WORKSHEET 3

03

Disclosure set and delivery ledger

Keep an unchanged original and record the exact version shared.

Document ID/version

Person concerned

Authorized scope

Redaction approved if any

Recipient

Verified method

Access setting

Sent date

Receipt

Related guidance: [Choose the verified delivery method](#)



WORKSHEET 4

04

Access and incident review

Do not use privacy cleanup as a reason to destroy relevant evidence.

Active link/authorization

Permitted audience

Expiry/review date

Record-retention question

Suspected incident

Facts preserved

Official contact

Next action

Related guidance: [Respond to a suspected mistake or scam](#)



READINESS REVIEW

Check the file before using it

REVIEW EACH ITEM BEFORE MOVING ON

- ☐ Each working figure or statement is linked to an identifiable document.
- ☐ Missing information is marked as unverified rather than estimated as fact.
- ☐ The exact question and the person or organization able to answer it are identified.
- ☐ The current document version and any conflicting version are preserved.
- ☐ Independent deadlines and the source of each deadline have been checked.
- ☐ The final written response has been compared with the original question.

What still needs attention

Open fact or decision, who can resolve it, and the source needed

Completion standard. The working file is complete when the important facts are supported, the next action is assigned and any unresolved issues remain clearly visible. A completed checklist does not establish coverage, entitlement or legal compliance.



ACTION PLAN

Write down the next step

Choose the smallest useful next step. Make the request specific enough that the recipient can locate the record and explain or address the exact issue. Keep proof of what you sent and what came back.

The exact issue or request

Evidence IDs and document versions that support the request

Verified recipient and channel

Date sent and follow-up date

What response will resolve the issue, and what still needs professional review

Separate decisions. A courtesy follow-up date is not a legal deadline. A document request does not automatically pause another requirement. Do not sign, settle, move property or disclose sensitive records merely because a box on this page is complete.



REFERENCE GUIDE

Sources and scope

The linked official sources support the educational background. The forms and examples are original organization tools. Sources were checked on October 1, 2026; policies, procedures and law may change. Recheck the current source before relying on a rule.

[1] FTC: Recognize and avoid phishing

Unexpected requests should be checked through a known genuine contact route. Scope: General anti-fraud guidance; not a determination that a particular request is fraudulent.

<https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams>

[2] HHS: Consent versus authorization

HIPAA authorization and routine consent are distinct, with specified authorization elements. Scope: HIPAA does not govern every organization or every record.

<https://www.hhs.gov/hipaa/for-professionals/faq/what-is-the-difference-between-consent-and-authorization/index.html>

[3] HHS: Revoking authorization

Revocation has written-receipt requirements and limits, including prior reliance. Scope: No blanket instruction to revoke or claim that past disclosure can be undone.

<https://www.hhs.gov/hipaa/for-professionals/faq/can-an-individual-revoke-his-or-her-authorization/index.html>



REFERENCE GUIDE

More source notes

[4] FTC: Identity theft resources

Official resources explain protection and recovery steps for misuse of personal information. Scope: Free official help is available through the linked resource; no promise to erase records is made.

<https://consumer.ftc.gov/articles/what-know-about-identity-theft>

Keep the scope clear

No advice to hide relevant evidence

No universal refusal of insurer cooperation

No passwords or full identity numbers in worksheets

No destructive privacy cleanup