HIPAA Incident and Breach Assessment

One form per incident: what happened, is it a breach, who must be told, and by when

Start this form the day you learn of an incident. Discovery starts the 60 day clock.

What happened

Date and time it happened

Date and time discovered

Discovered by

Official told (date, time)

Short description (use client codes, not names)

Latest notice date (discovery + 60)

1. Contain and preserve

- ☐ Disclosure stopped
- ☐ Recipient deletion in writing
- ☐ Passwords reset, sessions ended
- ☐ Device located, locked or wiped
- ☐ Messages and logs preserved
- ☐ Police report (if theft)
- ☐ Insurer notified
- ☐ Attorney or IT consulted
- ☐ Vendor (BA) contacted

2. PHI, permission, exceptions and encryption

- ☐ PHI was involved
- ☐ Use or disclosure not permitted by HIPAA
- ☐ Exception 1: workforce, unintentional, good faith
- ☐ Exception 2: authorized person to authorized person
- ☐ Exception 3: recipient could not retain it
- ☐ Secured: encrypted to HHS guidance, key not compromised
- ☐ Secured: destroyed (shredded, or NIST SP 800-88)

Notes: which exception, or how the PHI was secured

3. Four factor risk assessment and conclusion

Factor (164.402(2))	Facts found	Points to low risk?
1. The PHI: types, identifiers, likelihood of re-identification		☐ Yes ☐ No
2. Who used or received it (relationship, obligations)		☐ Yes ☐ No
3. Was it actually acquired or viewed? (evidence)		☐ Yes ☐ No
4. How far the risk was mitigated (assurances, wipes)		☐ Yes ☐ No

- ☐ Not a breach (exception or secured PHI)
- ☐ Low probability of compromise (documented)
- ☐ Reportable breach: notify

4. Notifications

Individuals affected (number, states)

Client notice: method and date sent

HHS report: date filed (or annual)

Media (over 500 in a state?)

Business associate

State law checked: which, deadline

Law enforcement delay

5. Mitigation, sanctions and changes

Mitigation and changes made (dates)

Sanctions or retraining

Decided by (privacy or security official)

Date

Reviewed by (attorney, if any)

Date

Keep this form, the evidence and copies of every notice for at least six years, outside client records.

A form to organize your assessment, not legal advice. Federal and state deadlines apply; get advice early.

Free printable from Lotus & Tulip · lotustulip.com/hipaa-breach-notification-for-therapists.html

HIPAA Incident and Breach Assessment

One form per incident: what happened, is it a breach, who must be told, and by when

FILLED EXAMPLE · fictional practice, people, numbers and dates

What happened

Date and time it happened	Date and time discovered	Discovered by	Official told (date, time)
03/08/2027, 4:40 pm	03/09/2027, 8:15 am	L. Brandt (office asst.)	03/09/2027, 8:30 am

Short description (use client codes, not names): Superbill for C-118 emailed to client C-204 (address autocomplete)

Latest notice date (discovery + 60): 05/08/2027

1. Contain and preserve

- [x] Disclosure stopped
- [x] Recipient deletion in writing
- [ ] Passwords reset, sessions ended
- [ ] Device located, locked or wiped
- [x] Messages and logs preserved
- [ ] Police report (if theft)
- [x] Insurer notified
- [x] Attorney or IT consulted
- [ ] Vendor (BA) contacted

2. PHI, permission, exceptions and encryption

- [x] PHI was involved
- [x] Use or disclosure not permitted by HIPAA
- [ ] Exception 1: workforce, unintentional, good faith
- [ ] Exception 2: authorized person to authorized person
- [ ] Exception 3: recipient could not retain it
- [ ] Secured: encrypted to HHS guidance, key not compromised
- [ ] Secured: destroyed (shredded, or NIST SP 800-88)

Notes: which exception, or how the PHI was secured: No exception: recipient is a client and could keep the email. Email not encrypted to the recipient.

3. Four factor risk assessment and conclusion

Factor (164.402(2))	Facts found	Points to low risk?
1. The PHI: types, identifiers, likelihood of re-identification	Name, DOB, member ID, 3 dates, mental health diagnosis code	☐ Yes ☑ No
2. Who used or received it (relationship, obligations)	Another client, known, no link to C-118, cooperative	☑ Yes ☐ No
3. Was it actually acquired or viewed? (evidence)	Opened and viewed (recipient replied about it)	☐ Yes ☑ No
4. How far the risk was mitigated (assurances, wipes)	Deletion confirmed in writing 03/09, 9:20 am	☑ Yes ☐ No

- [ ] Not a breach (exception or secured PHI)
- [ ] Low probability of compromise (documented)
- [x] Reportable breach: notify

4. Notifications

Individuals affected (number, states)	Client notice: method and date sent	HHS report: date filed (or annual)
1 (Texas)	Told in session 03/11; mailed 03/12	Filed 03/15/2027 (not waiting)

Media (over 500 in a state?)	Business associate	State law checked: which, deadline	Law enforcement delay
No (1 person)	None	TX 521.053: AG notice n/a (under 250)	None

5. Mitigation, sanctions and changes

Mitigation and changes made (dates): Autocomplete off 03/09; superbills only via portal from 03/10; risk analysis updated

Sanctions or retraining: Retrained 03/10, documented

Decided by (privacy or security official)	Date	Reviewed by (attorney, if any)	Date
D. Okafor, LPC	03/12/2027	J. Ruiz, attorney (fictional)	03/12/2027

Keep this form, the evidence and copies of every notice for at least six years, outside client records.

A form to organize your assessment, not legal advice. Federal and state deadlines apply; get advice early.

Free printable from Lotus & Tulip · lotustulip.com/hipaa-breach-notification-for-therapists.html

First 24 Hours and Incident Log

Twelve things to do when something goes wrong, plus a log of every incident and breach

In the first 24 hours

- [ ] 1. Write down what happened, when, and who knew first. Today may be your discovery date.
- [ ] 2. Stop it getting worse: recall, retrieve, lock or wipe, reset passwords, end sessions.
- [ ] 3. Ask any known recipient to delete it and confirm that in writing.
- [ ] 4. Preserve evidence: keep sent messages, screenshots and logs. Do not wipe devices yet.
- [ ] 5. Tell your privacy or security official now, by phone, and note the time.
- [ ] 6. Call your cyber or malpractice insurer if your policy requires prompt notice.
- [ ] 7. Theft: file a police report. Ransomware: call IT support, and consider the FBI.
- [ ] 8. If a vendor is involved, ask for the details in writing and check your BAA.
- [ ] 9. List every affected client and every type of information exposed.
- [ ] 10. Check the exceptions and encryption, then start the four factor assessment.
- [ ] 11. Calendar the 60 day outer limit and any shorter state law deadline.
- [ ] 12. Enter it on the log below, even if it turns out not to be a breach.

Breach and incident log

Discovered	What happened (codes, not names)	People	Outcome	Clients told	HHS told	Initials
03/09/2027	Superbill emailed to wrong client	1	Breach: notify	03/12/2027	03/15/2027	DO

One line per incident, including ones that were not breaches. Outcome: not a breach, low probability (documented) or breach. The first row is a fictional example. Breaches of fewer than 500 people go to HHS no later than 60 days after the end of the calendar year; you may report sooner.

A form to organize your assessment, not legal advice. Federal and state deadlines apply; get advice early.

Free printable from Lotus & Tulip · lotustulip.com/hipaa-breach-notification-for-therapists.html

L&T

Lotus & Tulip

Liked this free printable?

The complete, ready to print version is here:

Therapy Progress Notes and Intake Templates

Fillable PDF, 20 pages: SOAP, DAP and BIRP notes, intake, treatment plan and safety plan

Holiday sale on Etsy until Dec 2: about $7.36, was $9

Get it on Etsy

etsy.com/listing/4607261084 | instant digital download

See every page first: lotustulip.com/therapy-progress-notes-and-intake-templates.html

More free printables: lotustulip.com/free-tools.html

Lotus & Tulip printables. Personal and professional use with your own clients or students.