Security Risk Analysis

HIPAA Security Rule worksheet for a solo or small therapy practice. 45 CFR 164.308(a)(1)

Write down where client information lives, what could go wrong, how likely, how bad, and what you will do.

Practice and scope

Practice _____ Security official (prepared by) _____ Date _____

Locations in scope (office, home, remote staff) _____ Version _____ Next full review _____

1. Where electronic client information (ePHI) lives: tick all

- ☐ EHR or practice software
- ☐ Telehealth video
- ☐ Email
- ☐ Cloud storage or drive
- ☐ Texts on a phone
- ☐ Laptop or desktop
- ☐ Phone or tablet
- ☐ Backups, USB drives
- ☐ Scanner, fax, copier
- ☐ AI scribe or transcription
- ☐ Billing, clearinghouse
- ☐ Home office or remote work

2. Risk register: one threat and weakness per row

Where (asset)	Threat	Vulnerability	Current safeguards	L	I	Risk	Action, owner, due

3. Scales: L = likelihood, I = impact, Risk = L x I

Likelihood in the next year: 1 unlikely, 2 possible, 3 likely or it has already happened.
Impact: 1 minor (few clients, quick fix), 2 moderate, 3 serious (many clients, notes, or days without records).
Risk: 1 to 2 low, 3 to 4 medium, 6 to 9 high. Every medium and high row needs an action, owner and date.

4. Addressable safeguards: tick each one in place

- ☐ Encryption on devices
- ☐ Encryption in transit
- ☐ Automatic logoff
- ☐ Security reminders
- ☐ Log in monitoring
- ☐ Password management
- ☐ Contingency plan tests
- ☐ Integrity checks
- ☐ Device movement record

For any not ticked: why it is not reasonable, and the alternative you use

_____

Risk analysis completed by _____ Date _____ Risk plan approved by _____ Update early if _____

Never write passwords, account numbers or client names on this page. Fix high risks first.

Security Risk Analysis

HIPAA Security Rule worksheet for a solo or small therapy practice. 45 CFR 164.308(a)(1)

FILLED EXAMPLE · fictional practice, people, systems and dates

Practice and scope

Practice	Security official (prepared by)	Date
Juniper Hollow Therapy, PLLC	R. Okafor, LMFT (fictional)	11/10/2026

Locations in scope (office, home, remote staff)	Version	Next full review
Office suite 2B, home office, admin works remotely	2026 v1	11/2027

1. Where electronic client information (ePHI) lives: tick all

- [x] EHR or practice software
- [ ] Cloud storage or drive
- [x] Phone or tablet
- [ ] AI scribe or transcription
- [x] Telehealth video
- [x] Texts on a phone
- [x] Backups, USB drives
- [x] Billing, clearinghouse
- [x] Email
- [x] Laptop or desktop
- [ ] Scanner, fax, copier
- [x] Home office or remote work

2. Risk register: one threat and weakness per row

Where (asset)	Threat	Vulnerability	Current safeguards	L	I	Risk	Action, owner, due
Work laptop (notes, EHR, email)	Theft or loss from car or home	Disk not encrypted before this review	Login password, locks after 5 min	2	3	6	Turn on full disk encryption: RO, 11/14
Business email	Phishing, account takeover	No two step login on email account	Spam filter only	3	3	9	Turn on MFA on all accounts: RO, 11/12
Phone (texts, EHR app)	Lost or stolen phone	Client names show on lock screen	Passcode, remote wipe turned on	2	2	4	Hide previews; move texts to EHR: 11/20
EHR (vendor hosted, BAA)	Vendor outage or ransomware	No offline list of client contacts	Vendor backups, BAA on file	2	3	6	Monthly encrypted export: RO, 11/30
Telehealth from home office	Session overheard	Shared wall, no sound masking	Door closed	2	2	4	Noise machine and headset: RO, 11/21
Admin's home computer	Malware, family member access	Shared family PC, one login for all	Antivirus	2	3	6	Practice laptop for admin: 12/15
Old laptop in office closet	Lost during disposal or reuse	Drive never wiped	Closet is locked	1	2	2	Wipe, recycle, keep certificate: 1/10/27

3. Scales: L = likelihood, I = impact, Risk = L x I

Likelihood in the next year: 1 unlikely, 2 possible, 3 likely or it has already happened.
Impact: 1 minor (few clients, quick fix), 2 moderate, 3 serious (many clients, notes, or days without records).
Risk: 1 to 2 low, 3 to 4 medium, 6 to 9 high. Every medium and high row needs an action, owner and date.

4. Addressable safeguards: tick each one in place

- [ ] Encryption on devices
- [x] Encryption in transit
- [x] Automatic logoff
- [x] Security reminders
- [x] Log in monitoring
- [x] Password management
- [ ] Contingency plan tests
- [ ] Integrity checks
- [x] Device movement record

For any not ticked: why it is not reasonable, and the alternative you use

Device encryption due 11/14 (row 1); first restore test 11/30; integrity checks: EHR vendor

Risk analysis completed by	Date	Risk plan approved by	Update early if
R. Okafor, LMFT	11/10/2026	R. Okafor, owner	New system, incident, staff change

Never write passwords, account numbers or client names on this page. Fix high risks first.

Annual Risk Review

Ten checks once a year and after any big change, plus a log of every review and update

Annual review, in order

- [ ] 1. Update the list of every system, device and vendor holding client data.
- [ ] 2. Walk through how client information enters, moves and leaves.
- [ ] 3. Add new threats: phishing styles, new apps, AI tools, remote work.
- [ ] 4. Re-rate likelihood and impact for every row; add new rows.
- [ ] 5. Check last year's actions: done, late, or changed. Note why.
- [ ] 6. Test a restore from backup and time how long it takes.
- [ ] 7. Confirm MFA, encryption and auto lock on every device and account.
- [ ] 8. Remove access for anyone who left; review who can see what.
- [ ] 9. Confirm BAAs for every vendor in the register; log any new ones.
- [ ] 10. Sign, date and file this review; keep it at least six years.

Review and update log

Date	Why: annual or trigger	What changed	Risks added or re-rated	Actions done	By

Update early after a security incident or breach, a new EHR, telehealth, email or AI tool, a move or new office, a new hire or someone leaving, remote work starting, or a change in ownership. HHS says the rule does not set a frequency; many small practices review yearly.

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.