ClinicOps

FREE CHECKLIST

HIPAA Breach Response Checklist

From the first hour to the HHS report: every step, owner and federal deadline, a worked example and a readiness score.

This is the written plan your practice runs when patient information goes where it should not: a fax to the wrong number, an email to the wrong patient, a lost phone, a vendor's hack. It is built for a 1 to 10 physician practice where the privacy officer is also the practice manager. Print two copies and keep them with your privacy policies.

60 days
the outer limit to notify each patient, counted from the day of discovery, not the day you are sure
45 CFR 164.404(b)

63,966
breach reports affecting fewer than 500 people for 2022, and 91% came from health care providers
HHS report to Congress, 2024

$73,011
the most HHS can charge per violation in the three lower penalty tiers, 2025 adjustment
45 CFR 102.3

Start here

1. Today, 10 minutes: fill in the names below, then score your practice on page 2. Every No is a gap to close before an incident, not during one.
2. When an incident happens: start at page 3 and work down. Write a time next to each tick. The worked example on page 6 shows a finished record.
3. Count the deadlines from discovery: the deadline box on page 3 does the arithmetic. Day 60 is the limit, not the target.
4. Every January: review the breach log and send HHS last year's breaches of fewer than 500 people by Mar 1. The reasoning behind every line is in the full guide on clinicops.us.

WHO DOES WHAT IN YOUR PRACTICE

Privacy officer: _____

Backup privacy officer: _____

Owner or physician lead: _____

Counsel (name and phone): _____

IT support (name and phone): _____

Breach log kept at: _____

Today: could you run the 60-day clock?

#	Check (Yes only if you can show it in writing)	Rule	Circle
1	A privacy officer and a backup are named in writing.	164.530(a)	Yes / No
2	This plan, or your own, is written and filed with your privacy policies.	164.530(i)	Yes / No
3	Everyone on staff knows to tell the privacy officer the same day, and was trained on it.	164.530(b)	Yes / No
4	Every laptop and phone with patient data is encrypted, keys stored apart.	HHS guidance	Yes / No
5	One breach log with one owner, reviewed this January.	164.408(c)	Yes / No
6	Last year's breaches under 500 went to HHS by Mar 1, or there were none.	164.408(c)	Yes / No
7	Every vendor handling patient data has a signed agreement, and you know its notice window.	164.504(e)	Yes / No
8	A letter template with the five required elements is ready.	164.404(c)	Yes / No
9	You know your state's breach rule and its deadline.	State law	Yes / No
10	Sanctions for privacy violations are written and applied.	164.530(e)	Yes / No
11	Breach files are kept six years.	164.530(j)(2)	Yes / No
12	Counsel and IT contacts are written on page 1.	Practice	Yes / No

Count your Yes answers. 11 or 12: ready, so run a 15-minute misdirected-fax drill once a year. 8 to 10: exposed, so close every No this month, starting with the backup name, the log and the letter template. 7 or fewer: high risk. You could not prove a 60-day notice today, and under 45 CFR 164.414(b) proving it is your job.

Vendor gaps: track every agreement and notice window in the free **business associate agreement tracker**.

What a gap can cost: HHS civil money penalties per violation (2025 adjustment, 45 CFR 102.3)

Culpability	Per violation	Yearly cap
Did not know, and could not have known	$145 to $73,011	$2,190,294
Reasonable cause, not willful neglect	$1,461 to $73,011	$2,190,294
Willful neglect, corrected within 30 days	$14,602 to $73,011	$2,190,294
Willful neglect, not corrected	$73,011 to $2,190,294	$2,190,294

HHS has applied lower yearly caps to the first three tiers since 2019 as a matter of enforcement discretion (84 FR 18151). This is an operations checklist, not legal advice: your counsel decides whether an incident is a breach and what your state requires.

1. The first hour

- [ ] **Contain it: recall the fax or email, revoke the shared link, lock or wipe the device, change the password.**
  Whoever finds it acts first. How far you limit the damage is factor 4 of the risk assessment.
- [ ] **Tell the privacy officer, and write down the date and time of discovery.**
  The breach counts as discovered on the first day any workforce member other than the person who caused it knew or should have known (164.404(a)(2)).
- [ ] **Open the incident record below with a reference number. Keep it where only the privacy officer and owner can see it.**
  The practice carries the burden of proof that it notified or that no breach occurred (164.414(b)).
- [ ] **Preserve the evidence: fax confirmation, sent email, access log, the recipient's reply.**
  You need it for factors 2 and 3, and for the file you keep six years.
- [ ] **Do not promise anything to the recipient or the patient yet. Ask the recipient to delete or return it and to confirm in writing.**
  A signed attestation of destruction is the strongest mitigation evidence.

Incident record (chart numbers or reference codes only, never names or diagnoses)

Incident reference: _____ Date and time discovered: _____

Discovered by (role): _____ Privacy officer told at: _____

What happened, one line: _____ Chart numbers or count: _____

People affected, by state: _____ Vendor involved? Who?: _____

Your deadline box

Line	How to get it	Your date
A. Day 0	The date in the record above	_____
B. Day 60	Line A plus 60 calendar days. Patient letters, and media and HHS if 500 or more, by this day.	_____
C. Target mailing date	Aim for line A plus 30 days or sooner. Without unreasonable delay is the real standard.	_____
D. Days left today	Line B minus today's date. Under 15: escalate to the owner today.	_____
E. Under 500 people	HHS report by Mar 1, 2027 for 2026 breaches; Feb 29, 2028 for 2027; Mar 1, 2029 for 2028.	_____
F. Police hold	Written request: the period it states. Oral request: no more than 30 days unless a written one follows (164.412).	_____

2. Days 1 to 5: is it a breach?

Any use or disclosure the Privacy Rule does not permit is presumed to be a breach (45 CFR 164.402). Check the exclusions first, then the encryption, then write the four-factor assessment.

- [ ] **Exception 1: an unintentional, good-faith access by a workforce member acting within their authority, not used or shared further.**
- [ ] **Exception 2: an inadvertent disclosure between two people both authorized at this practice or business associate, not used or shared further.**
- [ ] **Exception 3: a good-faith belief that the person who received it could not have kept it.**
- [ ] **Encryption: the device or file was encrypted to the HHS standard and the key or password was not lost with it and is stored apart.**
  If so, it is not unsecured information and no notice is owed. Document the check either way (HHS guidance on unsecured PHI).

Four-factor risk assessment (45 CFR 164.402)

Factor	Question to answer in writing	Your finding
1. Nature and extent	Which identifiers and how much clinical detail? How easily could someone re-identify the person?	
2. Who received it	Is the recipient itself bound by HIPAA, such as another provider?	
3. Acquired or viewed	Was it actually opened, read, kept, copied or forwarded?	
4. Mitigation	What assurances do you hold, and in what form? Signed and dated?	

Decision (circle): NOTIFY or LOW PROBABILITY OF COMPROMISE: _____

Signed by and date: _____

3. By day 60: notify

Who to notify, and by when

Who	When it applies	Deadline	Rule
Each affected patient	Every breach of unsecured protected health information	Without unreasonable delay, no later than 60 calendar days after discovery	164.404
Prominent media in the state	More than 500 residents of one state or jurisdiction	Same 60-day limit	164.406
HHS, 500 or more	500 or more people	With the patient letters, inside 60 days, online portal	164.408(b)
HHS, under 500	Fewer than 500 people	Within 60 days after the end of the calendar year of discovery	164.408(c)
Your practice, from a vendor	Breach at a business associate	Within 60 days of the vendor's discovery, with names	164.410

- [ ] **Letter in plain language, first-class mail (email only if the patient agreed to electronic notice).**
  164.404(c)(2) and (d)(1)
- [ ] **It says what happened, with the breach date and the discovery date.**
- [ ] **It lists the types of information involved (name, date of birth, address, diagnosis and so on).**
- [ ] **It tells the patient what to do to protect themselves, and what you are doing to investigate, limit harm and prevent a repeat.**
- [ ] **It gives a toll-free number, email, website or postal address for questions.**
  The five elements are listed in 164.404(c)(1).
- [ ] **Missing addresses: under 10 people, another written notice or a call; 10 or more, website home page or major media for 90 days plus a toll-free number live 90 days.**
  164.404(d)(2)
- [ ] **Under 500: entered in the breach log with the decision and the letter date; 500 or more: HHS portal report sent with the letters.**
  164.408(b) and (c)
- [ ] **The cause is fixed, the people involved retrained, and any sanction applied and written down.**
  164.530(b), (e) and (f)
- [ ] **The file is complete: record, assessment, letters, proof of mailing, HHS receipt. Kept six years.**
  164.530(j)(2)

Worked example: a completed record

A two-physician family practice. Sample data, chart numbers only.

Field	Entry
Incident and discovery	INC-2026-07. Tue Nov 3, 2026, 2:40 pm, front desk lead, when the receiving office called
What happened	Referral packet for chart #A-10442 faxed to a number one digit off; it reached another physician office. 1 person, 1 state, no vendor
Containment	Recipient asked to shred; signed attestation of destruction received Wed Nov 4, 9:15 am
Factors 1 to 4	1: name, date of birth, one visit note. 2: another HIPAA-covered provider. 3: viewed only to spot the error. 4: attestation on file
Decision and dates	Low probability of compromise, signed by privacy officer and owner Nov 5. Day 60 would have been Jan 2, 2027. Logged
Fix	Top 20 referral fax numbers saved as presets, cover sheet updated, front desk retrained Nov 10
If one fact changes	Sent to a retail business, or no attestation: notify chart #A-10442 by Jan 2, 2027 and log it for the Mar 1, 2027 HHS report

When it goes wrong

If this happens	Do this	Rule
You learn of it weeks late, from a patient	Use the date someone on staff knew or should have known. Notify at once and record why it was late.	164.404(a)(2)
A vendor tells you on its day 55	Do not wait for your own day 60: mail as soon as you have the names. Check the vendor's window in your agreement.	164.410
You cannot get a count yet	Give HHS an estimate and file an addendum later. Letters may go in more than one mailing.	164.404(d)(1)
Police ask you to hold notice	Get it in writing with the period. If oral, record the official's name; the hold ends after 30 days without a written request.	164.412
The patient has died	Write to the next of kin or personal representative if you have the address.	164.404(d)(1)(ii)
Ransomware or hacking	Presumed a breach unless you can show a low probability of compromise. Counsel and IT the same day.	164.402
Staff looked up a neighbor's chart	Not an exception: not in good faith. Notify, sanction and document the sanction.	164.530(e)
Over 500, spread over states	Media notice only where more than 500 residents of one state are affected; letters and HHS regardless.	164.406
Your state has a shorter clock	Follow the stricter rule. California licensed clinics: state and patient within 15 business days.	Cal. HSC 1280.15

Sources

Checked against the original source on Nov 18, 2026. Rules and figures change: confirm anything time-sensitive on the source page.

1. 45 CFR 164.400 to 164.414, Breach Notification Rule (eCFR text current as of Nov 13, 2026) (2013, as amended). law.cornell.edu/cfr/text/45/164.404

2. 45 CFR 164.530, training, sanctions, policies, six-year retention (current). law.cornell.edu/cfr/text/45/164.530

3. 45 CFR 102.3, HHS civil monetary penalty table, 2025 adjustment (current Nov 2026). law.cornell.edu/cfr/text/45/102.3

4. HHS OCR, Annual Report to Congress on Breaches of Unsecured PHI for 2022 (GovInfo) (issued Feb 14, 2024). govinfo.gov/content/pkg/CMR-HE1-00196246/pdf/CMR-HE1-00196246.pdf

5. HHS, Submitting notice of a breach to the Secretary (reviewed Nov 2026). hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.htm

6. HHS, Guidance to render unsecured PHI unusable, unreadable or indecipherable (2013). hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

7. California Health and Safety Code 1280.15 (current). leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&se

Where this checklist stops

It tells you what to do on the day. Here is what paper cannot do for you:

- **It cannot notice an incident: someone has to know to tell the privacy officer the same day.**
- **It cannot remind anyone of day 60 or Mar 1: those dates live on paper until someone puts them on a calendar with an owner.**
- **It cannot train the team, write your policies, or check that every vendor has an agreement.**
- **It cannot cover the privacy officer's vacation week, which is when incidents go unlogged.**

Practice Controls: an SOP library a new hire can run on day one, a recurring task board, license and compliance calendars, and the cash controls that stop leakage.

Book the free 20-minute Chaos Audit >

It is a diagnostic call, not a sales call: we walk back the last thing that slipped, put an hours or dollar figure on it, and you leave with the first fix whether or not you hire us.

Not ready to talk? Score your practice in 3 minutes, or get more free tools and templates.
Follow ClinicOps for one useful fix a week: LinkedIn | YouTube | X | Instagram | Facebook