Palo Alto Health Labs

Incident and Breach Response — Small-Practice Action Card

Not legal advice. Not a compliance certification.

Reader-facing one-page copy

Use your approved response plan. This card supports escalation; it does not determine a legal breach or satisfy every federal/state rule. Do not wait for a breach decision to address an active incident.

Incident label: _____ First observed date/time + zone: _____
Response lead / approved contact route: _____
Technical responder: _____ Privacy/security lead: _____
Counsel / alternate contact route: _____

1. Protect care and contain the incident

☐ Activate the approved downtime/care-continuity workflow; report immediate care risks to the clinical lead.

☐ Alert the response lead promptly using a known-clean route if ordinary email/chat may be affected.

☐ Have authorized technical responders isolate affected systems/accounts or stop an exposed integration, coordinating care continuity and evidence preservation. For suspected ransomware, CISA recommends network isolation; powering off can lose volatile evidence. Do not improvise a wipe/reinstall. [3]

2. Preserve evidence and a timeline

☐ Record observations, affected system labels, actions, actors and timestamps with zones. Separate known facts from guesses.

☐ Ask responders to preserve relevant logs, messages, access records and volatile evidence using approved restricted storage; document collection/handling. Do not copy patient data into ordinary email or this card.

☐ Preserve original artifacts; do not delete suspected messages or reset/rebuild systems without responder direction. Coordinate urgent containment rather than delaying it for perfect evidence. [3]

3. Escalate internally and assign legal review

☐ Engage privacy/security leadership, management and counsel promptly; follow plan/contract routes for vendor, insurer and specialist support.

☐ Assign an owner to track applicable contractual and legal reporting requirements immediately—not after the investigation ends.

☐ Give counsel/reviewers facts about data types, recipients, possible access/acquisition and mitigation. HHS's breach analysis includes those factors; an incident is not automatically a legally determined reportable breach. [1]

4. Determine notifications and recover under ownership

☐ Have the accountable privacy/legal team document the breach assessment, applicable laws/contracts, affected parties, required recipients, deadlines and responsible sender. This card supplies no universal deadline or exemption.

☐ Coordinate required notifications without waiting for every fact; counsel should assess timing and available information. Under HIPAA, breach notifications can involve individuals, HHS and sometimes media, while business associates notify covered entities. Applicability differs. [1]

☐ Recover through authorized responders, verify integrity/clinical continuity, retain the decision record and assign corrective actions. Do not declare “no breach” because service is restored.

Next action / owner / next update: _____

Book a free 30-minute audit
For planning discussions—not an emergency-response contact or promised response service.

Separate source and editorial appendix — not on one-page card

Official pages opened/read 2026-11-07 PST:

[1] HHS Breach Notification Rule <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>: definition/presumption, risk-assessment factors, exceptions, recipient categories and documentation. This card does not reproduce notification thresholds or deadlines; those require applicable-law review. An impermissible use/disclosure of PHI is generally presumed a breach unless the applicable analysis demonstrates low probability of compromise or an exception applies; the card must not imply notification is optional merely because an incident is still being investigated.

[2] HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>: procedures for identifying/responding to suspected/known incidents, mitigation, documentation and contingency planning.

[3] CISA StopRansomware Guide <https://www.cisa.gov/stopransomware/ransomware-guide>: authorized-response context for isolation, out-of-band communications, volatile evidence and coordinated recovery. Ransomware-specific advice is not a generic instruction to power off every device.

Review flags: counsel must customize jurisdiction/role-specific notification triggers, deadlines, contracts, patient-record obligations and law-enforcement/insurer escalation routes. State laws, FTC applicability and practice-specific policy were not researched or determined; no promise this card satisfies all federal/state rules. No patient notice is drafted here. Clinical lead must approve continuity wording; technical lead must approve containment instructions. An active incident needs the practice's actual response contacts, not the marketing CTA. No evidence that PAHL provides incident response is asserted.

The primary CTA is planning copy, not an emergency assistance promise.

Limits

No PAHL capability, certification, outcome or delivery promise is asserted.

Not legal advice.

No booking URL, availability or free-call deliverables have been verified.