Breach-Response Runbook — Template

Wire this in before launch, not during an outage. Engineering guidance, not legal advice — confirm specifics with counsel.

THE FIRST HOUR (every security incident)

- ☐ **Detect and timestamp.** Record who first knew and when — this is your 'discovery' date and it starts the 60-day clock. Page the on-call lead.
- ☐ **Contain.** Isolate affected systems, revoke compromised credentials and tokens, block the access path. Stop the bleeding before investigating.
- ☐ **Preserve evidence.** Snapshot logs, access records, and system state before you change anything. You will need them for the risk assessment.
- ☐ **Convene the team.** Incident lead, engineering, security, privacy/compliance, and counsel. Open one incident record everyone writes to.
- ☐ **Classify severity.** Does it touch PHI? Which systems, which patients, how many, which states? Note any business-associate or vendor involvement.
- ☐ **Hold law-enforcement exceptions in mind.** A written LE request can delay notice; an oral one buys only a documented 30 days (45 CFR 164.412).

THE 60-DAY CLOCK (if PHI is involved)

- ☐ **Apply the safe harbor first.** Was the PHI encrypted-to-standard or destroyed? If 'secured', no breach notice is owed — document why.
- ☐ **Run the four-factor risk assessment.** Nature of PHI · who received it · actually acquired/viewed? · mitigation. Presumed a breach unless low probability — and you bear the burden of proof.
- ☐ **Write it down and keep it 6 years.** An undocumented 'it wasn't a breach' is a lost argument in an audit.
- ☐ **Notify individuals ≤ 60 days.** Plain language, 5 required elements. 10+ unreachable → substitute notice (90-day web posting or media + toll-free line).
- ☐ **At 500+ in one state: add media + HHS now.** Notify prominent state media and the HHS Secretary contemporaneously. Under 500: log for the annual HHS report.
- ☐ **If you are a business associate:** notify the covered entity fast — your BAA likely shortens the 60 days to 5/10/30. Identify affected individuals.
- ☐ **Not under HIPAA?** A direct-to-consumer app may owe the FTC Health Breach Notification Rule: individuals + FTC ≤ 60 days; FTC ≤ 10 business days at 500+.

THE ONE TEST BEFORE LAUNCH

Pick your worst plausible incident and walk it end to end on paper: who is paged, what is your discovery date, who owns the four-factor assessment, who drafts and sends notices, which regulator applies to this data flow, and what does your business-associate contract demand and by when? If any answer is 'we'd figure it out then', the runbook is not ready. Decide it now, while no clock is running.