GUIDE

Incident Response Plan and Tabletop

What this is	Who is called, in what order, what gets preserved, who notifies whom and on what clock — plus the tabletop exercise script that proves the plan works.
It assumes	You hold confidential records. Every organization in this sector does.
Change before use	The notification obligations, which depend on what data you hold and in which state — confirm them with counsel and write them into section 4 before you rely on this.

THE CALL LIST AND THE LOG ARE THE SPREADSHEET

This document explains the sequence and why each step is in it. **The working parts are the accompanying spreadsheet** — the call list with alternates and a checked date, the notification register your counsel fills in, the event log used live, and the tabletop record.

Print the event log. The first hour is not the time to look for a file.

The plan's one job

On the worst morning — ransomware on the case management system, a stolen laptop, a staff member's credentials phished — the plan's job is to replace improvisation with a sequence. Everything below is designed to be usable by a stressed person at 7 a.m.: names, phone numbers, an order of operations, and the two rules people break under pressure.

THE TWO RULES

Preserve before you fix. Do not wipe, reimage, or delete anything until evidence is preserved — what happened and to whose data determines your legal obligations, and destroying the evidence destroys your ability to answer.

Nobody communicates externally except the named voice. No staff posts, no individual replies to affected people, no statements — until the response lead and, where engaged, counsel approve the communication.

1. Roles — names and numbers

Role	Person	Backup	Phone
Response lead (declares an incident, directs the response)			

Role	Person	Backup	Phone
Technical lead (contains, preserves, investigates)			
Communications voice (the only external voice)			
Records/compliance lead (notification obligations)			
Counsel (engage early for anything touching client data)			
Cyber insurer hotline (policy #, and note: many policies require notice before costs are incurred)			
IT provider / key vendors			

2. First 24 hours

1. **Report.** Anyone who suspects an incident reports it immediately to the response lead — hour or day, no triage by the reporter. Late reporting is the failure mode; the plan states plainly that reporting is never punished.
2. **Declare and log.** The response lead opens the incident log: time, reporter, what is known. Every action from here is logged with a time.
3. **Contain.** Technical lead isolates affected systems — disconnect, disable accounts, block — using the systems inventory to find everything connected.
4. **Preserve.** Before remediation: image or snapshot affected systems where feasible, export relevant logs, photograph screens if that is what is available. Preserve first, then fix.
5. **Engage.** Counsel and the cyber insurer, per the numbers above, for any incident plausibly touching client, personnel, or financial data.
6. **Assess scope.** What systems, what data categories (use the inventory's sensitivity column), what people, what period.

3. Days 2–30

- Eradicate and recover: rebuild from clean sources, restore from backups (the tested restore — this is why it was tested), rotate credentials broadly.
- Determine notification obligations — section 4 — and execute them on their clocks.
- Track everything in the log: decisions, times, who was told what.

4. Notification obligations — complete with counsel before relying on this plan

Write here, as plain instructions with clocks and addresses: the state breach-notification requirements that apply to you; regulator and licensing notifications your program rules require; contractual notice obligations in county and funder agreements (many contain 24–72 hour clauses — pull them from the award inventory);

HIPAA obligations where applicable; and insurer notice requirements. This section is the reason the plan needs counsel's review once — after that, the 7 a.m. reader just follows it.

5. Afterwards

- A written post-incident review within [30] days: timeline, what worked, what did not, and system changes — through the corrective-action protocol, so the fixes are verified later.
- Board notified per its policy; the incident summary goes to the quality committee.

6. The tabletop — 60 minutes, twice a year

A plan that has never been exercised is a document, not a capability. Script: the facilitator reads the scenario in stages; the named roles say what they would actually do; the facilitator writes down every gap.

1. **Scenario, stage 1:** Monday 7:40 a.m. — a case worker reports the case management system is showing a ransom screen. What happens in the next thirty minutes? Who is called, in what order? (Watch for: does anyone preserve before fixing?)
2. **Stage 2:** The technical lead finds the backups also encrypted — except the offline copy from Thursday. What is lost? Who decides whether to restore?
3. **Stage 3:** A county program manager emails asking whether their referrals are affected. Who answers, and what may they say today? (Watch for: anyone but the named voice answering.)
4. **Stage 4:** The insurer asks for the incident log and the systems inventory. Can we produce them?
5. **Close:** every gap found goes on the corrective-action log with an owner. Date the plan's next revision.

Published by The CARES Collaborative, a program of Knotts Family Services, Inc., for adaptation and use by charitable and community-serving organizations. No registration, no fee, no attribution required. This document is a working template, not legal, tax, or accounting advice — the requirements that apply to your organization are confirmed by your own counsel, auditor, and licensing authority. Version 1.0 · August 2026 · carescollaborative.org/open-shelf