

AFTER-ACTION REPORT AND IMPROVEMENT PLAN

Sample Dental Group (made up) · Ransomware: the Monday morning lockout

Oct 8, 2026 · Facilitator: Alex Sample, Example Security Partners

1 HANDLED WELL	2 PARTLY	1 GAP	5 ACTION ITEMS
-------------------	-------------	----------	-------------------

SUMMARY

The team worked through "Ransomware: the Monday morning lockout" in 4 stages. 1 was handled well, 2 partly, and 1 showed a gap. Participants: Dr. R. Example (Executive decision-maker); Morgan Sample (Incident lead); Example IT Services on-call (Technical lead); Jamie Example (Communications lead); Robin Sample (Finance lead); Dr. T. Sample (Associate dentist).

OBJECTIVES

- Check that the front desk and the office manager know who is in charge and who to call in the first hour.
- Test how the practice keeps seeing patients when the schedule and X-ray systems are down.
- Find gaps in the incident response plan, the call list and the backups.
- Agree improvements, each with an owner and a date.

STAGE BY STAGE

Stage	Situation	Result	What the team did or missed
Stage 1 Monday 7:15 a.m.	The front desk cannot open today's schedule in the practice management system. In operatory 3, the X-ray imaging PC shows files ending in .lockd, and a text file on the shared drive demands payment within 72 hours. The first patients arrive at 8:00.	Handled well	Front desk unplugged the imaging PC in two minutes and called Morgan, who declared Level 3 and started the log.
Stage 2 7:50 a.m.	Example IT Services says the practice management server and the backup drive in the back office are both encrypted. The cloud backup from Sunday night looks intact. Twenty-two patients are booked today, and email still works on phones.	Partly	Group text worked, but it took 40 minutes to find the insurer's hotline and policy number.
Stage 3 11:00 a.m.	The attackers email Dr. Example a sample of 50 patient records, with names, dates of birth and dental insurance IDs, and say they will publish everything unless they are paid.	Gap	Two people wanted to reply to the attacker. Nobody knew who breach counsel was or when the HIPAA clock starts.
Stage 4 Day 2, 9:00 a.m.	A patient calls the front desk asking if their information is safe. A local TV station leaves a voicemail for Dr. Example. Restoring from the cloud copy will take three days, and the insurer's response firm is on site.	Partly	Dr. Example was the clear spokesperson, but there was no holding statement or front-desk script for patient calls.

STRENGTHS

The front desk reacted fast and correctly: isolate, leave powered on, call the office manager. The office manager took charge, declared a level and kept a written log from the first minute. The cloud backup exists and the IT provider knew how to reach it. Dr. Example was accepted by everyone as the only voice to patients and the press.

AREAS FOR IMPROVEMENT

The insurer's hotline and policy number were not on the call list, so the most important first call was delayed. The practice has no breach counsel lined up, and no one could say which notices HIPAA or Arizona law would require. The backup drive sits on the same network as the server it protects, and a full restore has never been tested. There is no prepared wording for patients who call.

IMPROVEMENT PLAN

#	Action	Owner	Due
1	Add the insurer's breach hotline and where the policy is kept to the first-hour card and the call list.	Morgan Sample	Oct 31, 2026
2	Print the next day's schedule as paper day sheets every evening, so patients can be seen if the system is down.	Morgan Sample	Nov 2, 2026
3	Confirm breach counsel through the insurer's panel and add them to the plan.	Dr. R. Example	Nov 13, 2026
4	Move the backup drive off the main network and test a full restore of the practice management server.	Example IT Services	Nov 30, 2026
5	Write a holding statement and a front-desk script for patient calls, reviewed by counsel.	Jamie Example	Dec 11, 2026

A tabletop exercise tests decisions and the plan. It does not test whether the technical steps work; restore tests and security assessments do that.