

Small Clinic Cyber Downtime Kit

EHR and network downtime planning for small clinics

USE AND PRIVACY BOUNDARY

Educational planning tool only. Not medical, legal, regulatory, emergency-management, or cybersecurity compliance advice.

Do not write protected health information, patient names, credentials, secrets, or live incident details on this worksheet.

Review with qualified personnel. Follow official guidance, organizational policy, and applicable law.

VERSION	SOURCE	LAST REVIEWED
2026-08-21	HealthSecurity.tech	2026-08-21

Purpose: Prepare the people, paper, communications, and recovery steps needed when an EHR, network, phone, or connected vendor service becomes unavailable.

Planning record

CLINIC / LOCATION

DATE

DOWNTIME PLAN OWNER

NEXT EXERCISE DATE

1. Before downtime

- ☐ Map scheduling, intake, records, phones, prescriptions, laboratories, referrals, billing, and vendor dependencies.
- ☐ Define who can activate and end downtime operations.
- ☐ Store current approved forms, job aids, contact lists, and procedures offline.
- ☐ Keep necessary paper, printer, label, power, and communication supplies available.
- ☐ Define service limits under approved organizational policy.

OFFLINE MATERIALS LOCATION

ALTERNATE COMMUNICATION CHANNEL

2. First hour

- [] Confirm the scope through approved technical and leadership channels.
- [] Activate the plan and notify staff using an independent channel.
- [] Prioritize patient-safety and time-sensitive operational dependencies.
- [] Start a timestamped situation log without PHI or sensitive technical details.
- [] Route external statements through the approved communications lead.

3. First day

- ☐ Schedule regular operational status checks.
- ☐ Track capacity, staffing, paper supplies, vendor status, and unresolved decisions.
- ☐ Communicate service availability and alternatives factually.
- ☐ Protect completed paper records under approved custody procedures.
- ☐ Escalate safety or emergency decisions to qualified personnel.

4. Paper workflow checklist

- ☐ Approved intake and identity process is accessible.
- ☐ Forms carry date, time, author, and appropriate record linkage under policy.
- ☐ A controlled collection point and custodian are assigned.
- ☐ Staff know which data must not be written on informal notes.
- ☐ A reconciliation method is defined before forms are used.

Note: This kit does not define clinical documentation requirements or treatment procedures.

5. Scheduling continuity

- ☐ Define how appointments are viewed, recorded, changed, and communicated.
 - ☐ Record which scheduling functions cannot be reproduced safely offline.
 - ☐ Prepare a method for later reconciliation and duplicate detection.
-
-

6. Prescription, referral, and laboratory continuity questions

- ☐ Which approved internal policies govern these workflows during downtime?
 - ☐ Which external services and communication paths are required?
 - ☐ Which qualified role decides whether work can proceed or must be deferred?
 - ☐ How will status be tracked and reconciled without exposing patient data?
-
-
-
-

7. Patient communications notes

- ☐ State confirmed operational facts only.
 - ☐ Provide available contact or service alternatives.
 - ☐ Do not include patient information or speculate about cause.
 - ☐ Set an honest next-update time when possible.
-
-
-

8. Restoration and reconciliation

- ☐ Validate systems and interfaces before routine use.
- ☐ Confirm leadership authorization to end downtime operations.
- ☐ Reconcile paper work under approved records policy.
- ☐ Detect duplicates, omissions, timing conflicts, and incomplete status.
- ☐ Retain the situation log and improvement decisions appropriately.

9. After-action review

REVIEW LEAD

REVIEW DATE

- ☐ What protected essential services?
 - ☐ Where did staff lack information, authority, supplies, or capacity?
 - ☐ Which assumption failed?
 - ☐ Which improvement has an owner and due date?
 - ☐ When will the revised process be retested?
-
-
-
-

USE AND PRIVACY BOUNDARY

Educational planning tool only. Not medical, legal, regulatory, emergency-management, or cybersecurity compliance advice.

Do not write protected health information, patient names, credentials, secrets, or live incident details on this worksheet.

Review with qualified personnel. Follow official guidance, organizational policy, and applicable law.