

Are We Actually Ready?

Seven checks that turn reassuring answers into operational confidence.

How to use it: Mark YES only when the answer is current, assigned, and supported by something you can show. If the group cannot agree, mark NOT SURE.

#	READINESS CHECK	YES	NO	NOT SURE
1	We have named the clinical and business functions that must keep working for patients to be seen, treated, contacted, and billed.	☐	☐	☐
2	Each critical function, system, and vendor relationship has one named accountable owner.	☐	☐	☐
3	We can produce current proof that backups, protections, contacts, and response plans are working as intended.	☐	☐	☐
4	Recovery has been tested recently, and we know what was restored, how long it took, and what failed.	☐	☐	☐
5	If systems go down at 8:00 a.m., staff know whom to call first, who can make decisions, and how to continue safely.	☐	☐	☐
6	Important unknowns and outside dependencies are documented instead of being carried in someone's head.	☐	☐	☐
7	Gaps that require a leadership decision, funding, or formal risk acceptance have an owner and a due date.	☐	☐	☐

YES: ____ / 7

NO: ____ / 7

NOT SURE: ____ / 7

The most important thing we cannot prove today:

Owner and date for the next action:

Questions to Ask Your IT Provider

A constructive conversation about scope, recovery, evidence, and shared responsibility.

Opening line: "We are not trying to audit your technical work. We need to understand what you own, what we own, and what evidence shows the practice can recover."

QUESTION	EVIDENCE TO REQUEST	NOTES / FOLLOW-UP
1. Exactly which systems and services are you responsible for - and what is excluded?	Current agreement, service inventory, responsibility list	
2. If several systems fail together, what is the recovery order and realistic recovery time?	Recovery runbook with priorities and time targets	
3. Where are our backups, how are they protected from ransomware, and who monitors failures?	Backup design summary, recent status, open exceptions	
4. When was the last restore test? What was restored, how long did it take, and what did not work?	Dated restore-test report or ticket	
5. How will a serious issue be detected and escalated after hours?	Alert path, on-call process, names and phone numbers	
6. Which devices, servers, email accounts, and cloud systems are protected - and which are not?	Current coverage report and exception list	
7. Who owns MFA, patching, administrator access, and prompt removal of former staff?	Latest compliance/access report and assigned owners	
8. What do you need from our practice, EHR, phone, internet, and other vendors to recover?	Dependency list and unresolved actions	
9. When and how will we be notified of a security event that may affect operations or patient information?	Incident communication process and contract terms	
10. What small evidence package can you send us every quarter?	Agreed report: coverage, exceptions, backup status, tests	

Listen for: Clear ownership, dates, exceptions, and test results. Treat "the backup runs every night" as a starting point - not proof of recovery.

Downtime at 8:00 a.m.

A practical worksheet for deciding what must continue before the pressure is real.

SCENARIO / SYSTEM UNAVAILABLE	DATE TESTED	DOWNTIME LEAD

PART 1 - WHAT MUST KEEP WORKING?

CRITICAL ACTIVITY	MAXIMUM ACCEPTABLE PAUSE	SAFE MANUAL WORKAROUND	WHAT THE WORKAROUND NEEDS	OWNER
Patient arrival, check-in, and scheduling				
Clinical records, orders, results, and documentation				
Phones, messages, and patient communication				
Prescriptions, referrals, labs, and imaging				
Billing, payments, authorizations, and claims				
Facility access, connected equipment, and supplies				

PART 2 - THE FIRST 60 MINUTES

TIME	ACTION
0-10 min	Protect patient safety; confirm the outage; name the downtime lead.
10-20 min	Call the assigned IT/vendor contacts; record the ticket and expected update time.
20-30 min	Activate safe manual procedures; tell staff what is unavailable and what to use.
30-60 min	Decide patient communication, schedule changes, and the time of the next leadership update.

The first workaround we need to test:	Owner and test date:

Responsibility Map

Make ownership visible across practice leadership, staff, IT, and outside vendors.

One rule: Every row gets one accountable owner. Write a person or organization - not "everyone" and not simply "IT."

ACTIVITY / DECISION	ACCOUNTABLE OWNER (ONE)	WHO DOES THE WORK?	BACKUP / ESCALATION	PROOF OR PLAN LOCATION
Define which operations must recover first				
Maintain the critical systems and vendor inventory				
Keep emergency contacts and escalation order current				
Protect and monitor endpoints, servers, email, and network				
Operate backups and respond to failed backup jobs				
Schedule and document recovery/restore tests				
Control MFA, administrator rights, onboarding, and offboarding				
Maintain and train staff on downtime procedures				
Lead incident decisions and internal communication				
Coordinate cyber insurer, legal, regulatory, and patient notice				
Approve funding or formally accept unresolved risk				

Rows without a clear owner:	The first ownership decision leadership will make:

A vendor can perform the work. The practice still needs to know who is accountable and where the proof lives.