



Cybersecurity Basics

ComplyClinic Playbook

Backup and Disaster Recovery Checklist

A practical checklist for identifying critical systems, backing them up, and testing recovery.

Audience: Small businesses that need to survive ransomware, accidental deletion, vendor outages, and hardware failure.

General educational resource only. This is not legal advice, certification advice, or a substitute for a formal security risk analysis, CMMC assessment, or incident response engagement.

Backups are not the same as recovery

A backup exists when data is copied. Recovery exists when you can restore the right data fast enough to keep the business running.

Many businesses discover too late that backups were incomplete, inaccessible, encrypted by ransomware, or never tested.

Identify critical systems

List systems that would stop operations: email, EMR, accounting, scheduling, file storage, ERP, CRM, website, phones, line-of-business apps, and network gear configs.

Assign each system an owner, recovery priority, recovery time objective, and recovery point objective.

Protect against ransomware

Maintain at least one backup copy that cannot be modified by normal user accounts or ransomware running in the production environment.

Use immutable storage, separate credentials, offline exports, or vendor-supported ransomware protection where appropriate.

Test restores

Test restoring a file, a folder, a mailbox, a device, and a critical business system. Document results and gaps.

A restore test is the moment backup marketing turns into operational reality.

Plan for vendor outages

Ask vendors how data is backed up, how long restores take, who authorizes emergency recovery, and how you export your data.

Cloud systems still need continuity planning. SaaS does not automatically mean your business has a tested recovery plan.

Document the emergency plan

Record who declares an incident, who contacts vendors, where backup credentials are stored, how staff communicate, and what workarounds are approved.

Quarterly checklist

Review critical system list, confirm backups are running, complete at least one restore test, update vendor contacts, and verify emergency credentials.

Next step: Schedule a backup and disaster recovery review to identify what would actually happen during an outage. Schedule now

Need help turning this into a practical roadmap? Book a free consultation at complyclinic.com.

ComplyClinic • Practical cybersecurity, compliance readiness, automation, app development, and AI governance support.