NJSBA PRACTICEHQ Affinity CONSULTING

KNOW YOUR OPTIONS – LOST DATA CAN BE RECOVERED (FOR A PRICE)

DRIVE FAILURE

A failed hard drive remains a real problem, but it is no longer the whole data-loss story. In a small or solo law firm, important information may be spread across laptops, desktops, phones, external drives, Microsoft 365 or Google Workspace, case-management software, accounting systems, e-signature platforms, cloud storage, scanned document folders, and old archive media. A single matter file may exist in several places, and each place may have different recovery rules.

That makes recovery both easier and harder than it used to be. Easier, because many cloud services keep deleted-item folders, version history, and administrative restore tools. Harder, because sync tools can rapidly copy a deletion or corrupted file across every device, and ransomware can target backups as well as live data. The question is no longer simply, "Can the drive be repaired?" It is, "Which copy is trustworthy, complete, recent, and restorable?"

TODAY'S DATA LOSS IS DIFFERENT

CLOUD SERVICES ARE CENTRAL, BUT NOT MAGIC.

Microsoft 365, Google Workspace, Dropbox, Box, iCloud, practice-management platforms, and similar services are highly resilient, but resilience is not the same as a firm-controlled backup. Retention windows, recycle bins, version history, and admin restore tools vary by service and license.

RANSOMWARE IS A RECOVERY PROBLEM AND A DATA PROBLEM.

A firm may be able to restore encrypted files and still have to determine whether data was copied, deleted, or altered before encryption began.

SSDS AND PHONES HAVE CHANGED PHYSICAL RECOVERY.

Modern solid-state drives, encrypted phones, and hardware-backed security features can make DIY recovery less useful and sometimes harmful. Encryption keys, device passcodes, and account credentials may be as important as the storage media itself.

BACKUPS NEED ISOLATION.

A backup that is always connected, writable by the same administrator account, or synchronized with live data may disappear during the same event that destroys the original.

TESTING MATTERS MORE THAN INTENTIONS.

A backup plan that has never restored a full mailbox, a case folder, or the accounting database is only a theory.

COMMON DATA LOSS CATEGORIES

For planning purposes, think in categories rather than devices.

- **Endpoint devices:** laptops, desktops, tablets, smartphones, and portable drives used by attorneys and staff.
- **Shared storage:** network-attached storage, file servers, shared folders, scanned-document repositories, and old external backup drives.
- **Cloud collaboration:** email, calendars, OneDrive, SharePoint, Google Drive, shared drives, Teams, Slack, and client portals.

- **Line-of-business systems:** case management, document management, billing, accounting, e-discovery, e-signature, and VoIP systems.
- **Archives and exports:** old PST files, PDF sets, discovery productions, departed-user mailboxes, database exports, and retired machines kept "just in case."

THE FIRST 15 MINUTES: WHAT TO DO WHEN DATA IS MISSING

Fast action helps, but rushed action can make recovery worse. The goal in the first few minutes is to stop the damage, preserve the best evidence of what happened, and avoid overwriting recoverable data.

- **Stop using the affected device or account.** Do not keep saving files, rebooting repeatedly, running repair tools, or trying random utilities.
- **If ransomware or malware is suspected, isolate first.** Disconnect the computer from Wi-Fi and wired networks. Do not start restoring files into an environment that may still be compromised.
- **If a mechanical drive clicks, grinds, or fails to spin normally, power it down.** Noise can mean physical damage. Continued attempts may turn a recoverable drive into an unrecoverable one.
- **Do not format, reinitialize, or reinstall.** Messages such as "drive not readable" or "needs to be formatted" are not instructions. They are warnings to pause.
- **Write down what happened.** Record the time, user, device, file path, cloud service, error message, and the last known good version.
- **Check safe recovery points before touching the original.** Look for recycle bins, version history, admin restore tools, recent backups, snapshots, and exported copies.
- **Escalate based on value and risk.** If the missing data affects active client work, accounting, deadlines, firm-wide access, or confidential records, involve the firm's IT provider or a qualified recovery professional before experimenting.

TYPES OF FAILURE

Different failures call for different responses. Treating them all the same is where many avoidable losses happen.

MECHANICAL, SPINNING DRIVES

Traditional spinning hard drives can suffer motor, platter, bearing, or read/write-head damage. Clicking, grinding, or repeated spin-up attempts point toward a physical problem. Shut the device down and consider a professional lab.

ELECTRONIC FAILURE

A power surge, bad enclosure, failed controller, or damaged port can prevent a drive from being detected. Recovery may be straightforward if the storage media is intact, but guessing with adapters and donor boards can cause more damage.

LOGICAL FAILURE

The storage device may work, but the file system, partition map, database, or application data is corrupted. Recovery often depends on avoiding writes and working from an image or backup, not the original device.

SOLID STATE DRIVES (SSD) AND NVME FAILURE

Solid-state drives often fail with little warning. TRIM, wear-leveling, encryption, and controller failures can limit recovery. If the data matters, stop using the drive quickly.

CLOID DELETION OR SYNC FAILURE

A user may delete or overwrite files locally, and the sync service may faithfully reproduce that change everywhere. Version history and admin restore windows can help, but they are time-limited and service-specific.

RANSOMWARE OR DESTRUCTIVE MALWARE

Backups may be encrypted, deleted, or sabotaged. Recovery should start with containment and trust decisions before restoration.

CHOOSING THE RIGHT RECOVERY PATH

Start with the least destructive option that matches the failure.

- **For a recently deleted cloud file:** check the user's trash, shared-drive trash, version history, admin restore tools, and any third-party cloud backup.
- **For an overwritten document:** look for version history in the application or storage platform before restoring an entire folder.
- **For a damaged external drive:** stop writing to it, avoid repair utilities, and decide whether the data value justifies professional imaging or lab recovery.
- **For a failed laptop:** determine whether the storage is removable and whether BitLocker, FileVault, or another encryption system is enabled. Keep recovery keys available.
- **For a failed phone or tablet:** check cloud backups, device management tools, photo/document sync settings, and account access before attempting device-level recovery.
- **For ransomware:** preserve logs, isolate systems, identify the cleanest restore point, verify backups in a safe environment, and rebuild trust before reconnecting restored systems.

BACKUP PREPARATION

A small firm does not need an elaborate enterprise program, but it does need a backup design that matches how the firm works. The backup plan should answer four practical questions: what is backed up, how far back can we go, how quickly can we restore it, and who knows how to do it?

INVENTORY CRITICAL DATA.

List the systems the firm cannot operate without: email, documents, case management, calendar, contacts, billing, accounting, scanned mail, templates, and password vaults.

SET PRACTICAL RECOVERY GOALS.

For each system, decide the acceptable amount of lost work and acceptable downtime. These are commonly called recovery point and recovery time objectives.

USE MORE THAN SYNC.

Sync keeps devices aligned; it is not the same as a backup. A bad change may sync just as efficiently as a good one.

KEEP AT LEAST ONE PROTECTED COPY.

Use backup storage that ordinary users and compromised endpoints cannot modify or delete. Depending on the platform, this may mean immutable, append-only, offline, or separately administered storage.

PROTECT CLOUD DATA TOO.

If the firm relies on Microsoft 365, Google Workspace, or a practice-management platform, confirm what native recovery is included, what must be enabled, and whether a separate cloud-to-cloud backup is appropriate.

SEPARATE BACKUP CREDENTIALS.

The account that performs backups should not be the same daily-use administrator account that reads email and installs software.

ENCRYPT BACKUPS AND KEEP RECOVERY KEYS ACCESSIBLE.

Encryption protects data, but a lost encryption key can make a perfect backup useless.

MONITOR BACKUP FAILURES.

Someone should receive and review alerts. Silent failure is common in small offices.

TEST RESTORES.

At least quarterly, restore a sample file, a folder, and one business-critical data set. Annually, test a larger scenario such as a departed user, lost laptop, or firm-wide file restore.

QUESTIONS FOR INTERVIEWING IT OR BACKUP PROVIDERS

- What exact systems are included and excluded?
- How often are backups taken, and how long are versions retained?
- Can users or malware delete the backups?
- Are backups isolated from the main administrator account?
- How are Microsoft 365, Google Workspace, case-management, billing, and accounting data protected?
- Can you restore one file, one mailbox, one matter folder, one user account, and the entire firm?
- How often do you perform restore tests, and will you provide written results?
- Where are encryption keys stored, and who can access them in an emergency?
- What happens if the IT provider is unavailable, out of business, or locked out?
- What is the expected recovery time for the firm's most important systems?

WHEN TO USE A PROFESSIONAL DATA RECOVERY COMPANY

Professional recovery is most appropriate when the original device is physically damaged, the data is high value, no good backup exists, or the failure involves encrypted or specialized storage. It is also appropriate when an attempted DIY recovery could overwrite the only remaining copy.

When evaluating a recovery company, look for criteria rather than brand names:

- Experience with the failed device type, including SSDs, NVMe drives, phones, RAID/NAS devices, and encrypted storage.
- A non-destructive evaluation process and a clear written estimate before work begins.
- Secure intake, tracking, and return or destruction procedures for client-sensitive media.
- A cleanroom or appropriate lab capability for physical drive work.
- A clear explanation of what was recovered, what was not recovered, and the format in which recovered data will be returned.
- No requirement that the firm approve expensive work before understanding the likely recovery scope.

Some companies specialize in recovering data from crashed hard drives, regardless of the cause. They are expensive, but not getting your data back may be even more costly.

- ADR Data Recovery;
- DriveSavers;
- Gillware;
- Ontrack Data Recovery; and
- Secure Data Recovery.