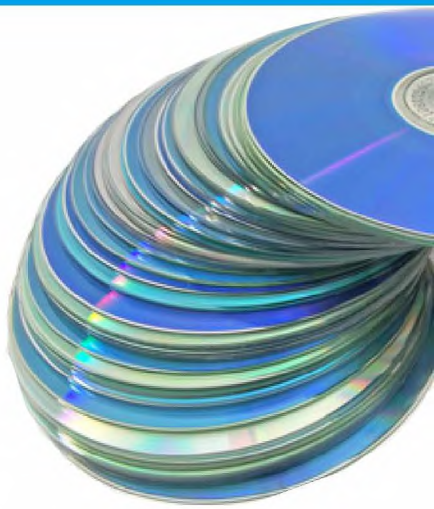
Getting
your Back-up



Jill Farrand,
Trust Account Supervisor,
Law Society Northern Territory

Regulation 40 of the *Legal Profession Regulations* requires law practices to make regular back-ups of trust account records maintained electronically, and additionally requires a complete set of back-up copies to be"kept in a separate location". Regulation 69 requires records to be kept for seven years. As the Northern Territory is prone to natural disasters of flood, fires, insect plagues and cyclones, it is also timely for law practices to consider a Data Disaster Recovery Plan (DDRP) and compliance with r40 and 69.

The practicality of a DDRP was recently reinforced after the 2010 Queensland devastating floods where many practices were unable to retrieve or reconstruct their trust records. Additional pressure was also placed on practices during this difficult time when clients requested access to their entrusted funds, and gave instructions for their matters to be suspended or withdrawn.

Computer trust records

Where law practices maintain trust records by way of a computerised system, the provisions in Regulations 40 and 69(2) apply.

Regulation 40 back-ups

The law practice must ensure:

(a) A back-up copy of all records required by this part is made not less frequently than once each month; and

(b) Each back-up copy is kept by the law practice; and

(c) A complete set of back-up copies is kept in a separate location so that any incident that may adversely affect the records would not also affect the back-up copy.

Regulation 69 keeping of trust records

(1) This regulation has effect for section 257 of the Act for the keeping in a permanent form of a law practice's trust records in relation to trust money received by the practice.

(2) The trust records must be kept for a period of seven years after:

(a) In the case of a trust record mentioned in paragraphs (a) to (m) of the definition "trust records" in section 235(1) of the Act – the only or the last transaction entry in the trust record; or

(b) In the case of any other trust record – finalisation of the matter to which the trust record relates.

Common mistakes

- Backing-upbywayofoverwriting a single monthly trust account file does not meet the obligations under r40.
- Maintaining back-ups to a server or hard drive held on site only also does not comply with r40.
- Not maintaining electronic records for seven years

In addition to on-site records, a complete set of back-ups must be maintained off site. Back-up files are to be maintained in such a way that they may be accessed and retrieved at any one time. Interpretations of similar provisions in other jurisdictions require law practices to maintain a set of unique monthly trust records for a period of seven years. This equates to 84 back up files at any one time. (12 monthly backups X 7 years = 84 separate and retrievable backup files). The following practice is acceptable to the Society.

Good practice

The Society recommends the following approach is adopted, to minimize the number of files:

- 12 unique files representing each month are to be maintained for any given reporting year.
- After the completion of the external examination, a single back-up file containing all transactions for the reporting year is made and

- The individual monthly files for the previous reporting period may then be deleted or over written by the monthly back-ups of the current period.

At the end of any given seven year period, this approach results a maximum of 18 back up files.

(six yearly backup files + 12 individual monthly files = 18).

Off site

The regulations require that a complete set of back-up copies be stored in a separate location from the law practice so that any adverse event impacting the practice will not also impact the back-up copies. When considering what is suitable off- site storage, practices ought to consider the likely incidents that may adversely affect records held at the practice, and ensure that the complete set of back-up copies is stored in such a location as to not be at risk of being adversely affected by the same incident.

DDRP under the Legal Profession National Rules

The requirement for off site storage will be similar under the proposed national legislationand rules.

A complete set of back-up copies is kept in a separate location so that any incident that may adversely affect the records would not also affect the back-up copy.(see *Legal Profession National Rules*Rule 4.2.12)

Back-up options

Practices have a number of options available for electronic off-site storage, from the simple to the complex. Importantly, the Society does not recommend or promote any particular storage option and suggest practices should consider the requirements of their practice, the limitations of various options, and likely "incidents that may adversely affect the records" located at the practice. Several of the more common options are briefly outlined below and may be divided into two rough groups; portable hardware options, or remote back-up options.

Portable back-up options

When considering portable options key things to consider:

- What is the life-span of the device (e.g. USBs are usually two years)?
- Can you incorporate regular trial data retrieval into our plan to check that the files remain accessible?
- Do you need a disaster proof vault to ensure that the disaster impacting the practice will not impact the device?
- Do you need an auxiliary back-up option?

Examples:

- **External hard drives / USB sticks –** USBs have a short life-span
- **Monthly Tape –** Suitable for small to medium firms with low to medium monthly transactions
- **Burn to CD –** This medium has a longer life span than the devices mentioned above. Useful as a secondary auxiliary to external hard drives or a USB.

Remote back-up options

When considering remote back-ups practices should consider:

- The third party solution is reputable;
- The terms of the Service Level Agreement, particularly provisions for data security;
- What is the supplier's disaster recovery plan?
- Can the provider ensure that monthly trust account records are individually and uniquely stored?

Emailing a monthly file to the most relevant practitioner. This is a simple option, suitable to low volume monthly transaction. Files are held off-site and often outside of the jurisdiction. Practitioners are encouraged to be mindful of archiving features and changing providers (email addresses) to ensure seven years of transactions are maintained at all times.

Cloud backup is where trust account data is copied to a website and can be retrieved using logins from any location with an online computer. This may be a relatively an inexpensive option.

Data warehousing. A number of practices uselocal technology service providers which also offer data watehousing. Practices need to ensure files are not synchronised/over written in respect to trust account records

Online line accounting systems. Many software companies are increasingly moving to online hosting of their software and customer data storage. A number of practices are using the Law Institute of Victoria's online trust accounting system which not only meets all reporting and recording requirements, but is also compliant with r40 and r69.

Remember, if in doubt concerning any trust account obligations contact the Trust Account Supervisor at the Society.