



RU RMT 26 · GOOD BUSINESS PRACTICES

LECTURE 10 · DIGITAL LITERACY FOR PROFESSIONALS

File Management, Naming Conventions, File Formats and Cloud Platforms

Where your documents live, what they are called, what format they are in, and how they are backed up.

Block B — Digital Literacy for Professionals

Day 5 · Session 2

Ruhani College · Registered Massage Therapy Diploma Program · Brampton, Ontario

9 Days · 63 Hours · 7 Hours per Day | Aligned with FOMTRAC Inter-Jurisdictional Practice Competencies, CMTO Standards of Practice and CMTCA accreditation standards



Where This Lecture Fits

The least interesting lecture in the course, and the one that saves the most time.

Lecture 9 produced documents. Lecture 10 is about what happens to them: how folders are organised, how files are named, which formats to use for which purpose, where files are stored, and how they are backed up.

This matters more in a practice than it does at home. When a colleague covers for you, when an insurer requests documentation, when the CRA asks for substantiation, or when a client exercises their right of access under PHIPA, the question is always the same: can you find it quickly and is it intact?

Lecture 11 then covers digital communication, and Lecture 12 the security that protects everything discussed here.



Learning Outcomes

By the end of this lecture you will be able to:

- Explain why electronic file management matters in a clinical business and what disorganisation costs.
- Apply hierarchical folder organisation and evaluate its advantages and limitations.
- Apply consistent naming conventions, including date-first naming and version control.
- Identify common file formats, their programs, and the advantages and disadvantages of each.
- Compare cloud storage platforms and identify the requirements that apply when client information is involved.
- Distinguish synchronisation from backup and implement a backup strategy that is verified.
- Apply retention and secure disposal practices consistent with PHIPA and CMTO record-keeping requirements.



Standards and Competency Alignment

Competency and regulatory basis

- **CMTO Record Keeping Standard:** records must be legible, complete, secure, retained for the required period and retrievable.
- **PHIPA, 2004:** a custodian must protect records against loss and unauthorised access, and enable client access and correction.
- **Canada Revenue Agency:** business records must be retained and be capable of substantiating income and deductions.
- **Information and Privacy Commissioner of Ontario:** guidance on cloud storage, encryption and secure disposal.

Why this matters in practice

- A record you cannot find is, for practical purposes, a record you do not have.
- Data residency and third-party access matter when a cloud provider holds personal health information.
- Synchronisation propagates deletions and corruption; only true backup protects against them.
- Retention periods are prescribed, and disposal before or after the period both create problems.



What We Will Cover Today

- Why computer organisation matters, and the cost of disorganisation
- Hierarchical folder organisation: pros, cons and guidelines
- Naming conventions: the two main methods and how to choose
- Version control and dating
- File formats: what they are and which to use when
- Web browsers and how the cloud is reached
- Cloud platforms compared, and the requirements for client data
- Synchronisation is not backup: the 3-2-1 rule
- Retention, archiving and secure disposal
- Building the folder structure for your practice



Vocabulary for This Lecture

- **Directory or folder** — a container that organises files within a storage device.
- **Naming convention** — an agreed, consistent pattern for naming files and folders.
- **File format** — the structure in which data is stored, indicated by the file extension.
- **Native format** — the format an application saves in by default.
- **Hierarchical organisation** — folders nested inside folders in a logical tree.
- **Version control** — tracking successive versions of a document so the current one is unambiguous.
- **Extension** — the suffix identifying the format, such as .docx, .pdf or .csv.
- **Portable format** — one that preserves appearance across systems, principally PDF.



Vocabulary for This Lecture

- **Lossy and lossless** — compression that discards data versus compression that does not.
- **Synchronisation** — keeping the same files identical across devices; changes propagate everywhere.
- **3-2-1 rule** — three copies, on two media, with one held off-site.
- **Retention period** — the length of time a record must be kept before disposal.
- **Cloud storage** — files held on a provider's servers and reached over the internet.
- **Backup** — an independent copy that is not changed when the original changes.
- **Data residency** — the country in which data is physically stored.
- **Secure disposal** — irreversible destruction of a record or the media holding it.



The Importance of Computer Organisation

There is no single correct structure. There is only a consistent one that everyone follows.

There is no one right way to achieve ideal folder organisation or naming. What matters is that a system exists and is applied. As a new employee, the first thing to identify is the configuration the business already uses — do not impose your own on top of it.

If naming conventions are intuitive and standardised, files can be found immediately. When an employee is absent and someone takes over their work, correct naming is not a convenience; it is what makes the handover possible at all.

The consequences of disorganisation are concrete: time lost searching, work duplicated because a file could not be found, the wrong version sent to a client, a document lost entirely, and — in a regulated practice — an inability to produce a record when it is properly requested.



What Disorganisation Actually Costs

Everyday costs

- Time lost searching, repeatedly, for documents that exist.
- Work redone because the previous version could not be found.
- The wrong version sent to a client, an insurer or an accountant.
- Files lost entirely when a device fails or a person leaves.
- Handover made impossible when someone covers for you.

Costs with regulatory weight

- Inability to produce a record when a client exercises their PHIPA right of access.
- Inability to substantiate income or a deduction to the Canada Revenue Agency.
- A record retained beyond its retention period with no disposal process, increasing exposure unnecessarily.
- A record disposed of before its retention period expires.
- Client information found in an unsecured location because there was no rule about where it belonged.



Hierarchical Folder Organisation

Advantages

- It is the most common method, so others will understand it.
- It allows quick, predictable access to information.
- Related items are stored together, which supports both work and archiving.
- It maps naturally onto how a business is actually structured.
- It scales: a new category becomes a new folder rather than a redesign.

Limitations

- It can be time-consuming to set up properly at the start.
- It can be difficult to restrict the number of files that accumulate in a folder.
- Where no guidelines are provided, users invent their own folder names and the structure fragments.
- A file that belongs in two categories has to be filed in one; use consistent rules rather than duplicating.
- Deep nesting becomes un navigable. Three levels is a sensible working limit.



Folder Organisation Guidelines

Each of these exists because of a specific failure it prevents.

- **Be consistent.** The same kind of thing is filed in the same place every time. Inconsistency is what makes a structure unusable to anyone else.
- **Structure folders in a logical sequence.** Group by function — finance, marketing, administration — rather than by date at the top level.
- **Do not create too many subfolders.** Every extra level is another decision to make when filing and another place to look when searching.
- **Keep the files in subfolders restricted.** A folder with two hundred items in it is a search problem, not a structure.
- **Do not use the Desktop as permanent storage.** It is often excluded from backup, it is visible to anyone who glances at the screen, and it has no structure at all.
- **Write the structure down.** A one-page diagram in your business plan means the structure survives you forgetting it.
- **Follow the conventions of any business you join.** Their system may not be your preference, but a second competing system is worse than an imperfect single one.



Two Naming Methods

Method	Pattern	Sorts by	Best for
Date-first	YYYY-MM-DD Description v01	Chronology	Anything where sequence matters: minutes, statements, agendas, correspondence
Category-first	Category Description YYYY-MM-DD	Subject	Reference material where you browse by topic rather than by date
Either way	Use the ISO date form YYYY-MM-DD	—	Removes all ambiguity between day-first and month-first conventions
Versioning	v01, v02, v03 — never 'final'	—	Anything revised more than once
Avoid	Spaces where systems may object; / \ : * ? " < >	—	These characters break on some systems and in some software

Pick one method, write it down as a rule with examples, and apply it without exception.



Writing a Naming Convention That Survives

A convention that is not written down is a preference, and preferences drift.

- State the pattern explicitly: what comes first, what separator is used, how dates are formatted, how versions are marked.
- Give three worked examples in the written rule. Examples communicate far more than a description.
- Use the ISO date format YYYY-MM-DD so files sort chronologically and 03-04-2026 is never ambiguous.
- Be descriptive but concise. A filename should tell you what the file is without opening it.
- Use leading zeros — v01 rather than v1 — so versions sort correctly past nine.
- Never use 'final'. Use a dated version and mark the approved one explicitly if you must.
- Never put client names in filenames stored outside your secure clinical system. Use a file number.
- Review the convention annually and after any occasion when someone could not find something.



Common File Formats and Their Uses

Format	Typical program	Use it for	Watch for
.docx	Word processors	Documents you will keep editing	Formatting can shift between applications
.pdf	Any reader	Anything sent out or signed: forms, receipts, reports	Not easily editable, which is usually the point
.xlsx	Spreadsheets	Models, budgets, projections	Formulas can break if opened in another suite
.csv	Any spreadsheet or system	Exporting and importing data between systems	Plain text only: no formatting, no formulas
.jpg	Image viewers	Photographs for marketing	Lossy compression; quality degrades on re-saving
.png	Image viewers	Logos, screenshots, graphics with text	Lossless; larger files than JPEG
.mp4	Video players	Client education and marketing video	Large files; check upload limits
.zip	Any operating system	Bundling several files for transfer	Encrypt if the contents are sensitive

General rule: edit in a native format, distribute as PDF, and export data as CSV.



Choosing the Right Format for the Job

Three rules cover almost every decision.

- **Edit in the native format.** Keep working documents in the format the application saves in, so nothing is lost between sessions.
- **Distribute as PDF.** Anything leaving your practice — a receipt, a policy sheet, a report — goes out as PDF so it appears the same everywhere and is not casually altered.
- **Move data as CSV.** When exporting from one system and importing into another, CSV is the common language. It carries no formatting and no formulas, which is exactly why it works.
- **Images: PNG for graphics, JPEG for photographs.** PNG is lossless and better for logos and screenshots; JPEG compresses photographs efficiently but degrades each time it is re-saved.
- **Archive in open formats.** A file you may need in ten years should not depend on a subscription you may no longer hold.
- **Compress before sending large sets.** And encrypt the archive if the contents are sensitive.
- **Never rename an extension to change a format.** It does not convert the file; it only makes it fail to open.



Web Browsers and Reaching the Cloud

Browsers

- A web browser is an application used to access websites; there are estimated to be well over two hundred in use, though a handful dominate.
- The main ones are Chrome, Safari, Edge, Firefox and Opera. Each supports extensions, saved passwords and synchronised bookmarks.
- Your practice-management software almost certainly runs in a browser, which makes the browser a clinical system.
- Keep it updated, limit extensions to ones you trust, and never save clinical passwords in a browser on a shared machine.
- Use a separate browser profile for business, so personal browsing and clinic access are cleanly separated.

Cloud platforms

- Cloud storage keeps files on a provider's servers, reachable from any device with credentials.
- The main consumer and business options are Microsoft OneDrive, Google Drive, Apple iCloud, Dropbox and Box.
- The benefits are access from anywhere, automatic synchronisation, version history and sharing without email attachments.
- The obligations are the important part when client information is involved — see the next slide.
- Cloud storage is not the same as your practice-management system. Clinical records belong in the latter; business documents belong in the former.



Using the Cloud When Client Information Is Involved

PHIPA does not prohibit cloud storage. It requires you to have taken reasonable steps, and to be able to say what they were.

- Use a paid business tier, never a free personal account. Business agreements provide the terms, controls and audit capability that consumer accounts do not.
- Establish where the data is physically stored. Data residency in Canada is a common requirement for health information and is the reason several practice-management platforms advertise Canadian data centres.
- Confirm encryption both in transit and at rest, and enable multi-factor authentication on every account.
- Understand the provider's access, breach notification and data return terms before you commit. Ask what happens to your data if you stop paying.
- Limit who has access, and remove access immediately when someone leaves.
- Keep a written record of these decisions. If a breach occurs, the question will be what reasonable steps you took, and a documented answer is worth a great deal.
- Where clinical records are concerned, prefer a purpose-built practice-management platform that addresses these requirements directly — covered in Lectures 13 and 14.
- Consult the Information and Privacy Commissioner of Ontario's current guidance rather than relying on a vendor's marketing claims.



Evaluating a Cloud Provider

01 Establish where the data is stored

Ask for the physical data centre location. Canadian residency is frequently required for health information and is a stated feature of several clinic platforms.

02 Confirm encryption in transit and at rest

Both, not one. Ask what standard, and get it in writing.

03 Check the access and subprocessor terms

Who at the provider can see your data, under what circumstances, and which other companies are involved.

04 Check breach notification obligations

How quickly will they tell you, and what will they tell you? You cannot meet your own notification duties without theirs.

05 Establish exit terms

How do you get your data out, in what format, and what happens to their copy? Ask before you need to leave.

06 Enable multi-factor authentication

On every account, without exception. This single control prevents the large majority of account compromises.

07 Write the decision down

What you asked, what you were told, and when. If a breach occurs, this record is your evidence of reasonable steps.



Synchronisation Is Not Backup

This distinction is the single most commonly misunderstood point in small business technology.

Synchronisation keeps the same files identical across your devices. If you delete a file on your laptop, it is deleted on your phone, your tablet and the server within seconds. If a file becomes corrupted, the corrupted version propagates. If ransomware encrypts your files, the encrypted versions synchronise everywhere. Synchronisation is a convenience feature and a single point of failure.

Backup is an independent copy that does not change when the original changes. A file deleted today can be recovered from last week's backup. That is the entire distinction, and it is the difference between an inconvenience and a catastrophe.

Most cloud providers offer limited version history and a recycle bin, which mitigates but does not replace backup. Assume you need a real backup unless you have specifically verified otherwise.



The 3-2-1 Rule

01 Three copies of anything you cannot lose

The working copy plus two backups. One backup is a single failure away from none.

02 On two different media or services

For example, an external drive and a cloud backup service. Two copies in the same place fail together.

03 One copy off-site

A fire, flood or theft at the premises must not take everything. Cloud backup satisfies this easily.

04 Automate it

A backup that depends on remembering will not happen during a busy month, which is exactly when you will need it.

05 Encrypt any backup containing client information

An unencrypted backup drive is a privacy breach waiting to be left in a car.

06 Verify quarterly

Restore one file and open it. This is the step everyone skips and the one that reveals a backup has silently been failing.

07 Document the arrangement

What is backed up, where, how often, who verifies it and when it was last tested.



Retention, Archiving and Secure Disposal

Retention

- Clinical records must be retained for the period specified by the CMTO's record-keeping requirements. Confirm the current period directly with the CMTO rather than relying on recollection.
- Business and tax records must be retained for the period the Canada Revenue Agency requires for substantiation.
- Different record types have different periods. Write a retention schedule listing each type, its period and its disposal method.
- Records of a minor typically attract a longer retention period. Check the current rule.
- Retaining everything indefinitely is not a safe default: it increases exposure without benefit.

Disposal

- Disposal must be secure and irreversible. Deleting a file does not remove the underlying data.
- For paper: cross-cut shredding or a certified destruction service with a certificate.
- For digital: secure erasure tools, or destruction of the media. Where the drive is encrypted, destroying the key is effective.
- Never dispose of a record that is subject to a complaint, an investigation or a legal proceeding.
- Keep a disposal log: what was destroyed, when, by whom and by what method.
- The same applies to any device leaving your control — sold, traded, recycled or returned under warranty.



Building a Retention Schedule

One table, listing every record type you hold. Write it once and review it annually.

- List the record type: clinical records, consent forms, financial records, tax filings, employment records, insurance policies, marketing material, correspondence.
- For each, state the retention period and the authority for it — CMTO requirement, CRA requirement, or your own business decision.
- State where each type is stored and in what format.
- State the disposal method for each: secure erasure, media destruction, cross-cut shredding, or certified destruction service.
- State who authorises disposal and who records it.
- Add a hold rule: nothing is disposed of while it is subject to a complaint, investigation or legal proceeding, regardless of its age.
- Confirm the current CMTO retention period directly with the College rather than relying on a course note or a colleague's recollection — requirements are periodically revised.
- Keep the schedule as an appendix to your business plan, and keep the disposal log with it.



A Workable Folder Structure for a Practice

A starting point to adapt, not to copy exactly. Keep it to three levels.

- **01 Business administration.** Registration and licences, insurance policies, lease and premises, equipment inventory, business plan and its versions.
- **02 Finance.** Bank statements by year, receipts by month, invoices issued, tax filings, projections and models.
- **03 Clients and clinical.** Where clinical records are held outside the practice-management system. Prefer to keep them inside it — see Lecture 14.
- **04 Marketing.** Logo and brand assets, website content, photographs, campaign material, printed collateral.
- **05 Professional development.** Certificates, course materials, QA documentation, self-assessment records.
- **06 Templates.** Every blank form, letter and document master, versioned. Nothing completed lives here.
- **07 Suppliers and contracts.** Agreements, warranties, service contracts, supplier correspondence.
- **99 Archive.** Closed years and superseded material, retained but out of the working structure.



The Test of a Good System

Could someone else run your practice for a week using only what you have written down?

That is the whole standard. If a colleague covering for you could find the schedule, the intake forms, the fee schedule, the policy sheet and the supplier contacts without phoning you, the system works. If they could not, it does not — regardless of how well it works for you personally.

The same test applies to every other system in this course. A business that exists only in the owner's head is fragile in exactly the way a solo practice can least afford, because the owner is also the person most likely to be unavailable through illness or injury.

Write the structure down, keep it with the business plan, and hand it to someone once a year to see whether they can use it.



Activity: Design and Build Your Folder Structure

Individually, on a computer. Allow 30 minutes.

Step 1 (10 minutes). On paper, design the folder structure for your future practice. It must accommodate: business administration, finance, marketing, professional development, templates, and any clinical documentation held outside your practice-management system. Do not exceed three levels of nesting.

Step 2 (10 minutes). Write your naming convention explicitly as a rule, with three worked examples. State whether you are using date-first or category-first, how you will format dates, how you will handle versions, and what you will never use in a filename.

Step 3 (10 minutes). Build the structure on your own device, place at least three real files into it using the convention, and then test it: ask a partner to find a named file in your structure without help. If they cannot, the structure or the convention is not intuitive.

A note on the exercise: there is no single correct answer. What matters is that it is consistent, that it is written down, and that someone covering for you could use it.



Taking This Into Your Living Business Plan

Add or revise the following sections of your plan after this lecture:

- Section 52 — Folder structure diagram for the practice, with the naming convention stated as a written rule.
- Section 53 — File format policy: what is stored as an editable document, what as PDF, and what is archived.
- Section 54 — Storage plan: where files live, which cloud provider, and the data residency position.
- Section 55 — Backup strategy under the 3-2-1 rule, including who verifies restores and how often.
- Section 56 — Retention schedule by record type, with disposal method and who authorises it.
- Section 57 — Continuity note: how a colleague covering for you would find what they need.



Common Errors and Examination Focus

- Using the Desktop as permanent storage, which defeats both backup and organisation.
- Inventing folder names ad hoc because no convention was written down.
- Using spaces, slashes or special characters in filenames in ways that break on other systems.
- Writing dates as 03-04-25, which is ambiguous. Use the year-month-day form.
- Naming versions 'final', 'final2' and 'final-really'. Use dated or numbered versions.
- Treating cloud synchronisation as backup. A deletion or a corruption propagates to every device within seconds.
- Storing personal health information in a free consumer cloud account with no business agreement and unknown data residency.
- Never testing a restore, then discovering during an incident that the backup has been failing for months.
- Disposing of records before the retention period expires, or keeping them indefinitely with no disposal process.



Self-Test Questions

Answer these before completing the worksheet for this lecture. They are ungraded and will be reviewed in class.

1. Give three consequences of poor file organisation in a clinical business, and state which of them has regulatory significance.
2. Write a naming convention as an explicit rule, with three worked examples, for a practice's financial documents.
3. Explain the difference between synchronisation and backup, and describe a scenario where the difference determines whether data is recoverable.
4. State the 3-2-1 rule and explain the specific risk each of the three elements addresses.
5. What questions would you ask a cloud provider before storing any document containing client information with them?



Key Takeaways

- There is no single correct structure; there is only a consistent one that is written down and followed.
- Hierarchical folders are the common approach: be consistent, keep it logical, and limit both nesting and file counts.
- Never use the Desktop as permanent storage.
- Use the ISO date format, use numbered versions with leading zeros, and never use 'final'.
- Edit in a native format, distribute as PDF, and export data as CSV.
- For client information in the cloud: paid business tier, known data residency, encryption, multi-factor authentication, and a written record of the decision.
- Synchronisation propagates deletion and corruption; only real backup protects you.
- Follow the 3-2-1 rule, automate it, encrypt it, and verify a restore every quarter.
- Retention periods are prescribed; disposal must be secure, logged and never during an active proceeding.



Texts and Professional Literature

- Sohnen-Moe, C. (2016). Business Mastery: A Guide for Creating a Fulfilling, Thriving Business, 5th ed. Books of Discovery. ISBN 978-1-882908-05-9.
- Benjamin, B. E. & Sohnen-Moe, C. (2013). The Ethics of Touch: A Guide to Creating a Professional, Safe and Enduring Practice, 2nd ed. Books of Discovery.
- Salvo, S. G. (2023). Massage Therapy: Principles and Practice, 7th ed. Elsevier. ISBN 978-0-323-87815-9.
- Fritz, S. & Fritz, L. A. (2021). Mosby's Fundamentals of Therapeutic Massage, 7th ed. Elsevier. ISBN 978-0-323-66183-6.
- Rattray, F. & Ludwig, L. (2000). Clinical Massage Therapy: Understanding, Assessing and Treating Over 70 Conditions. Talus Inc. ISBN 978-0-9685951-0-5.
- Braun, M. B. & Simonson, S. J. (2023). Introduction to Massage Therapy, 4th ed. Wolters Kluwer.
- Thompson, D. L. (2018). Hands Heal: Communication, Documentation and Insurance Billing for Manual Therapists, 4th ed. Wolters Kluwer.



Regulatory, Legislative and Standards Sources

- College of Massage Therapists of Ontario (CMTO). Standards of Practice — cmto.com/rmts/standards-and-rules
- CMTO Standards used throughout: Code of Ethics; Consent; Record Keeping; Advertising; Fees and Billing; Privacy and Confidentiality; Professional Boundaries; Infection Prevention and Control; Communication; Client-Centred Care.
- Regulated Health Professions Act, 1991 (RHPA), S.O. 1991, c. 18 — ontario.ca/laws
- Massage Therapy Act, 1991, S.O. 1991, c. 27, and O. Reg. 544/94 (General).
- Health Care Consent Act, 1996 (HCCA), S.O. 1996, c. 2, Sch. A.
- Personal Health Information Protection Act, 2004 (PHIPA), S.O. 2004, c. 3, Sch. A.
- Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
- Employment Standards Act, 2000 (ESA), S.O. 2000, c. 41 — ontario.ca/document/your-guide-employment-standards-act-0
- Canada Revenue Agency — business income, GST/HST, and employee versus self-employed guidance (canada.ca/cra).
- Federation of Massage Therapy Regulatory Authorities of Canada (FOMTRAC). Inter-Jurisdictional Practice Competencies and Performance Indicators (2016).
- Information and Privacy Commissioner of Ontario — guidance for health information custodians (ipc.on.ca).
- Canadian Anti-Spam Legislation (CASL), S.C. 2010, c. 23 — fightspam.gc.ca; Accessibility for Ontarians with Disabilities Act, 2005 (AODA).