dentalcorp

A guide on record keeping and protecting patient confidentiality & information

2021

CANADA'S BEST MANAGED COMPANIES

dentalcorp.ca

Table of Contents

Dental Record Keeping 101

The dental record (i.e. patient chart) is the official repository of all diagnostic information, clinical notes, treatment and patient-related communications that occur in the dental office, including instructions for home care, consent to treatment and finances.

Recording accurate patient information is essential to the practice of dentistry; diligent, timely and complete record keeping is fundamental to the delivery of quality patient care. A well-kept and maintained patient record provides invaluable data, which can be used to assess the quality of care that has been provided and to properly plan for treatment going forward.

Furthermore, the patient chart provides a means of communication between the treating practitioner and another clinician who may treat that patient in the future. Therefore, the dental record should contain enough information to allow another provider to understand the patient's experience in your office, i.e. what treatment was provided, what conditions have been diagnosed but remain untreated, together with the clinical justification for both.

What should the dental record contain?

First and foremost, the information contained in the patient chart should be clinical in nature. The following are examples of what is typically included in the dental record:

- General patient information, such as name, birth date, address, and contact information.
- Place of employment and telephone numbers (home, work, mobile).
- Appropriate evidence of informed consent.
- Diagnostic records, including radiographs and study models.
- Medication prescriptions, including types, dose, amount, directions for use and number of refills.
- Treatment plan notes.
- Patient complaints and resolutions.
- Laboratory work order forms.
- Referral letters and consultations.
- Patient noncompliance and missed appointment notes.
- Follow-up and periodic visit records.
- Post-op or home instructions.
- Conversations with patients dated and initialed (both in-office and on the telephone, even calls received outside the office).
- Patient-dentist correspondence, including dismissal letter.

Progress notes

Progress notes comprise a critical aspect of the patient's record. Because they are so essential for treatment continuity, progress notes should be completed during or immediately after each visit and must be reviewed and approved by the treating clinician. The level of detail required is both patient and treatment specific; however, progress notes should contain:

- The date of treatment.
- The treating clinician's identity.
- The materials and methods, including the type, amount, and result of any anesthetics used.
- Radiographs exposed and what they revealed.
- All recommendations, advice and any discussions regarding possible complications or outcomes.

Medical and dental histories

To allow for the provision of safe dental care, dental professional must ensure that all necessary and relevant medical information is obtained prior to initiating treatment. Medical and dental histories should be collected in a systematic manner, recording the patient's present state of health and any serious illnesses, conditions or adverse reactions in the past that could inform the patient's clinical management.

The patient chart must likewise include a notation of any significant dental history, such as an assessment of caries risk and periodontal health. Every patient is unique and the dental history should be considered together with the clinical examination when planning and sequencing of dental care.

General record keeping principles

- Chart entries should not be ambiguous or contain too many non-standard abbreviations.
- Handwritten entries should be legible, even to people unfamiliar with the provider's handwriting.
- All chart entries should be dated and recorded in permanent ink or an acceptable electronic format.
- All entries should be signed, initialed or otherwise attributable to the treating clinician, especially in clinics with multiple providers.
- X-rays and other diagnostic aids (e.g., study models) should be properly labelled, dated and the findings should be documented when the practitioner considers it appropriate.
- The overall treatment plan, treatment alternatives, any material risks or information and the estimated costs of treatment should be provided to each patient and/or legal guardian. This conversation should be recorded in the patient chart.
- In complex or difficult cases, a signed informed consent sheet should be obtained and kept.

Records and third-party payors

Dental records are also evidence of the work performed and could be necessary to get paid (e.g. by insurance companies). If the chart doesn't justify the claim submitted, an insurance company might refuse payment. This will certainly lead to an upset patient, and if there is a serious discrepancy between the progress notes and the code(s) submitted, fraud might be suspected. In these situations, insurance companies could audit your records or even report you to the College. Keeping good records helps avoid this unnecessary stress. For example:

- The date the service was provided and the code must align with the treatment recorded.
- A complicated extraction is not something that was difficult, rather it indicates a flap was raised and/or the tooth was sectioned.
- A PFM crown must have a lab receipt that confirms the materials used. If you provide a Zirconoia crown and accidentally submit the code for a PFM, you might be accused of insurance fraud or overbilling.

Never, never retroactively alter the patient chart

To avoid allegations of tampering, errors or incorrect information should never be erased or eliminated from the chart. Instead they should be struck out in such a way that the original notation is still readable. Electronic records must leave an audit trail that accomplishes the same result. Late entries should be clearly marked as such. In no circumstances should a clinician add to or correct a patient's chart after receiving a demand for compensation or notice of legal proceedings. Any changes made against that backdrop would be perceived as self-serving, perhaps even fraudulent.

Other things that should generally be omitted from the patient record include:

- Overt criticisms of care rendered by another clinician.
- Legal advice you received in relation to a patient complaint or claim for compensation.
- Insulting references to the patient or patient's friends and family.
- Subjective opinions that are not tied to other objectively measurable data, e.g., "the patient's blood pressure was really high."

When things go wrong, good records are your best friend

Beyond patient care, the dental record is important because it may be used as evidence in court or in a regulatory action to establish the diagnostic analysis that was performed and what treatment was rendered to the patient. A quality dental record can be used to respond to a patient complaint, in defense of allegations of malpractice, or to justify treatment in case of an audit by a third-party payor. In all these scenarios, information found in the record will help demonstrate that the diagnosis and treatment were reasonable and conformed to the relevant standards of care. If the patient chart is sparse or non-existent, the decision maker will be left to assess the credibility of the parties, knowing that the clinician was negligent at the very least in his or her record keeping duties.

What do I have to give to a patient when they request their "chart"?

Patients are legally entitled to access to their complete dental records and upon request, the dental office must provide the patient with a copy of all requested records in a timely fashion. This right is very expansive and includes records prepared by other doctors that the dentist may have received. Whether you are providing the records directly to the patient or transferring them to another clinician, as a general practice, you should not let the original files out of your control. The physical copy of original dental records (if kept in hard copy) is the property of the health care provider that created it.

How long do we have to keep dental records?

In general, clinical and financial records, as well as radiographs, consultation reports, and drug and lab prescriptions must be maintained for at least ten years after the date of the last entry in the patient's record. In the case of a minor, these records must be kept for at least ten years after the day on which the patient reached the age of eighteen years.

Patient Confidentiality

Patient information in a dental office is protected by laws, both federal and provincial, that strictly limit how such information can be collected, used, disclosed, and destroyed.

Staff come into contact with a wide variety of patient information in their day-to-day duties. Therefore, it is important for all staff at the dental office to understand the rules and their responsibilities when dealing with patient information. Failure to follow these rules can lead to serious consequences for the patient, the office, and the staff members alike.

What information is protected?

Virtually all personal information about a patient is protected, and includes such things as:

- Health information (medical/dental conditions, treatment history, etc.).
- Dental records (charts, radiographs, etc.).
- Identifying information (name, address, telephone number, health card number, etc.).
- Insurance and financial information (credit card numbers, invoices, benefit provider, etc.).

Even the mere fact that the individual is a patient of the office, including the identity of their treatment providers, is considered protected information!

Consent to collect, use and disclose information

In general, a dental office must have the consent or agreement of the patient in order to collect, use, or disclose their personal information for a particular purpose. More importantly, a patient can withdraw their consent at any time.

Consent can be implicit or explicit

Implicit consent is when consent can be inferred from the patient's actions or surrounding circumstances. For example, a patient who sits in the dental chair and opens their mouth when asked by the dentist is implicitly consenting to being examined by the dentist.

Explicit consent is when consent is given actively and openly by the patient. This is the form of consent usually required when dealing with patient information or providing dental treatment.

In many cases, explicit consent can be given verbally or in writing; however, some cases require explicit written consent from the patient. For example, under Canada's Anti-Spam Legislation, the office requires a patient's explicit written consent to contact them by email or text message.

For more information about CASL, see **http://www.crtc.gc.ca/eng/internet/anti.htm**

All new and existing patients must sign the office's forms, which sets out how the office will deal with their personal information. This is an example of explicit consent.

Using patient information

Once patient information has been collected, it should only be used for the purposes for which it was originally provided. Staff should only use patient information for legitimate purposes related to the patient's dental care and treatment with the office, such as scheduling appointments, discussing treatment with the patient, submitting insurance claims and billing, referrals to other practitioners, etc.

Similarly, staff must only access patient information in the course of their duties for legitimate purposes. For example, "snooping", such as looking up a patient's age or marital status out of curiosity, or searching for patients on the internet and social media, is not permitted.

Staff are accountable to patients for how their personal information is used and accessed at the office. It is important to note that many software programs used in a dental office track this use and access.

Duty of confidentiality

All staff in the dental office owe a duty of confidentiality to every patient of the office, both past and present. This means that they must keep confidential all patient information that they become aware of.

Staff should never disclose any personal information about a patient to anyone outside of the office, unless the disclosure is:

- in the course of their duties at the office
- for a legitimate purpose, and
- with the consent of the patient or required by law.

The duty of confidentiality lasts forever – even after the patient leaves the office or dies, or after the staff member leaves the office.

Examples

- Do not discuss patient information with friends or family, including the identity of patients at the office.
- Do not disclose patient information to anyone other than:
  - the patient
  - the patient's legal guardian (for minor children)
  - the patient's authorized substitute decision maker (e.g. power of attorney for an incapable adult), or
  - a person / organization for which the patient has provided explicit consent (e.g. insurance provider)

Dealing with families

Regardless of the relationship, the duty of confidentiality is applied strictly. For example, staff must not provide information about one spouse to the other spouse without the first spouse's explicit consent.

Cases involving divorced, separated, or blended families can pose challenges, and staff should be cautious when disclosing information in these circumstances. Mature minors may also be entitled to confidentiality of their personal health information.

If in doubt, confirm with the patient or speak to the Compliance Team before disclosing the information!

Access to patient information

Patients have a right to access their personal information kept at the office; however, the physical records remain the property of the dental office. Original records should never be provided to the patient. Dentists are required to provide copies of a patient's dental records to the patient or their designate upon request.

Protection of patient information

Staff must handle patient information in a manner that keeps it protected and secure. Staff should be cautious when handling patient records and when sending or sharing patient information in the course of their duties to ensure that it is not accidentally disclosed to unauthorized persons.

Examples

- Do not leave patient records or other documents with patient information lying around or in plain view where they can be seen by others in the office; use folders to cover paper records wherever possible.
- Lock your computer and turn on the screen saver when you step away from your desk.
- Securely shred any documents containing patient information after the expiry of the retention period (documents with patient information should never go in standard garbage or recycling!).
- Store patient records in a location that is kept secure and locked.
- Do not send patient health information by unencrypted email.
- Do not store patient health information on portable electronic devices, unless encrypted.
- Wherever possible, speak to patients in a private area regarding their treatment.
- Ensure all office computer systems are password protected and encrypted.
- Try to speak quietly with patients at the front desk, so that their personal information is not overheard by other patients in the office.

Contacting patients

Patients provide their contact information (e.g. address, phone number, email address) for purposes related to their dental treatment. It is generally acceptable to contact a patient by phone or email to schedule appointments, provide treatment or financial information, or for similar related purposes.

According to Canada's Anti-Spam Legislation, the dental office can only contact patients via text or email if they have given their explicit written consent to receive communications from the office.

In addition, unencrypted email and text messages should only be used for non-sensitive information, such as appointment reminders and general office announcements (e.g. newsletters).

Protecting Patient Information in and outside of the Office

The following policy will:

- Define safeguards for protecting patient records.
- Identify best practices for protecting paper and electronic records.
- Describe reasonable practices for protecting personal information outside of the office.

Health Care Providers have legal, professional and ethical obligations to maintain their patients' personal information in confidence and protect their privacy. This means that health information custodians must implement adequate safeguards to minimize the risk of any unauthorized use, access or disclosure of personal information. Safeguards are a combination of policies, processes, practices, and technologies that are intended to protect personal information. Regardless of how personal health information is recorded—whether on paper or electronically—appropriate and reasonable safeguards are necessary to ensure that privacy is protected, and confidentiality is maintained.

Dental professionals have an ethical obligation to respect patient confidentiality. Across Canada, laws and regulations exist that require dental professionals to protect the personal health information of their patients. Privacy legislation in every Province requires dental professionals to take reasonable measures to protect patients' personal information from risks of unauthorized access, use, disclosure and disposal, and sets out the consequences for violation. In 2018, the Information and Privacy Commissioner of Ontario released a guidance document entitled "Privacy by Design," which instructs healthcare workers to "anticipate, identify and prevent privacy-invasive events before they occur." The OIPC urges doctors and their teams to do this by "build[ing] in the maximum degree of privacy into the default settings for any system or business practice". This sentiment has been echoed by Privacy Commissioners and Ombudsmen across Canada. The bar is a high one.

Protecting records in the office

Patient records must be handled in a secure manner from the time the records are created to the time they are disposed of, regardless of the format upon which the information is stored.

The following measures must be incorporated into the implementation plans for safeguarding patient records and any other personal information stored in the clinic. Note that a combination of measures may be required during the transition from paper-based patient records to Electronic Dental Records (EDRs) where both methods of record-keeping may be maintained in parallel.

Basic safeguards

Staff working in dental practices should:

- Receive formal training in requirements for the protection of information and demonstrate that they know and understand required policies, procedures and best practices in the office.
- Lock doors and cabinets where patient records are stored.
- Wear building passes/photo ID if issued.
- Query the status of strangers.
- Know whom to inform if suspicious behaviours are noticed.
- Not tell unauthorized individuals how security systems operate.
- Immediately inform the privacy officer in the office of any actual or suspected breach of security.
- Sign confidentiality agreements that specify obligations and expectations, including repercussions for inappropriately collecting, using, or disclosing personal information.

Paper records should be:

- Formally booked out from the normal filing system.
- Tracked, if transferred, by confirming that the records arrived at their specified destination.
- Returned to the filing location as soon as possible after use.
- Stored securely/locked within the clinic or office.
- Placed in a location where members of the public cannot view the contents.
- Not left unattended at any time.
- Held in secure storage, off the floor, with clear labelling.
- Protected from heat and water sources to prevent damage.
- Kept on-site wherever possible. If the records must be taken off-site, they must be kept secure at all times and logged in and out on a leger that identifies who logged them out, for what purpose, when logged out and when logged back in.

Office IT requirements:

Whether or not the office has paper or Electronic Dental Records, certain network and information technology requirements must be met whenever there are one or more computers utilized in the practice. At a minimum:

- All computers, servers, networks and electronic devices should be configured by certified IT professionals.
- All software on devices must be appropriately licensed and kept up-to-date with security patches and updates.
- All storage devices must be encrypted, and password protected. This includes storage media.
- Measures need to be in place to ensure the security of data in motion and/or at rest.
- If remote access is to be permitted, the IT/Network administrator must ensure appropriate protections are in place, and that access can only be achieved through a secure and encrypted VPN connection. Data should, wherever possible, remain on the host network system with the remote system able to view that data and execute necessary commands on the host.
- Portable devices should not be used to store personal health information. If it is absolutely necessary to do so on a portable device, the user must log that device out and must ensure that it is shut down and securely stored when not in use. The IT administrator must install security software on all portable devices allowing them to disable the device and wherever possible, wipe the data if the device is lost or stolen.
- Strong passwords must be used at all times and must be changed periodically.
- Wherever possible, two-factor authentication should be used for passwords.
- Passwords must be revoked immediately upon termination or resignation of a staff member.
- Networks must be secured by industry-standard anti-virus programs with virus definition files updated frequently, as well as hardware/software firewalls configured appropriately by an IT professional competent and qualified to set up and maintain networks containing private health information.
- The network administrator must ensure that data is backed up regularly and that the back up and recovery system works by regularly testing the system and backing up test data.
- The network administrator must ensure that disaster recovery/business continuity plans are in place and are tested regularly to ensure they work.

With Electronic Dental Records (EDRs), staff should:

- Receive formal training on the legal and operational requirements, policies, and procedures to safeguard private health information.
- Receive formal training on all IT systems and programs they will need to rely on or utilize to perform their jobs.
- Only be granted the lowest level of access to perform their necessary job function. In other words, staff should only be provided the needed access to carry out their assigned duties.
- Log out of computer systems or applications when not in use or unattended.
- Keep workstations positioned away from public view and access.
- Not share an assigned user ID and password with others. Every staff member who needs access to EDR information must be given and must use their unique ID and password to access the EDR system.
- Not write down passwords.
- Not share passwords with others.
- Not use shared accounts.

EDRs should provide:

- A unique user ID and password for every authorized user.
- Password complexity
  - a. 12 or more characters.
  - b. Lock account after 5 unsuccessful attempts.
- Access to patient information on a "need to know" basis under a roles-based access model that determines whether the user has the necessary authorization and permissions.
- Audit trails to track when a patient record is accessed, by whom, including date and time, as well as any and all changes made to a record.
- Enforced password changes at regular intervals of every 12 months.
- Ability to easily manage user accounts (create, modify, revoke).
- Password protected screensaver or auto logout after a period of inactivity to avoid unauthorized viewing.

Protecting personal information outside the office

There are times when dental professionals and their staff may need to work with personal information while travelling, at home, or at another location. This includes transporting records by car or airplane, working from home, and attending meetings or conferences. The personal information may be stored in paper records or on portable electronic devices (such as laptops, CDs, DVDs, external hard drives, USB storage devices, handheld electronic devices and smartphones); however with the movement toward Electronic Dental Records (EDRs) and other forms of electronic communication, dental professionals and their staff are also able to connect to their office network, and therefore may have access to sensitive personal health information from anywhere in the world.

Under Privacy Legislation, dental professionals must implement reasonable safeguards to reduce the risks associated with working with personal information remotely while travelling, at home, or at another location.

Guidelines for conversations outside the office:

- Avoid discussing personal information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants, etc.
- When in transit, avoid using cell phones to discuss personal information, as such conversations maybe intercepted or overheard.
- If a staff member regularly works from home, a dedicated phone line with password-protected voicemail is recommended.

Guidelines for personal information stored on paper or portable electronic devices when outside the office:

- Remove records containing personal information only when it is absolutely necessary for performing job duties. If possible, take a copy with the originals left in the office. Take only the minimum amount of personal information required.
- Require all staff to obtain approval from their supervisor before removing records containing personal information from the office.
- All paper records should be contained in a locked briefcase or file container.
- When travelling by car, keep records locked in the trunk before the start of a trip—don't put them there once at the destination. Do not leave records unattended, even if they are stored in the trunk. Car trunks are no less accessible to thieves than the front seats.
- Do not view records in public places where they may be viewed or accessed by unauthorized individuals(e.g., at cafes or on public transit).
- Do not leave records open for view in hotel rooms; they should be kept in the hotel safe.
- Upon returning to the office, immediately replace records containing personal information to their original storage location.
- Securely destroy any copies that are no longer required.

Guidelines specific to personal information stored on paper-based records when outside the office:

- Use a sign-out sheet to document who is removing a record, the name of the individual whose personal information is being removed, and the date the record is being removed as well as the date the record is returned.
- If the records are large, consider using a courier to transport it to the destination.
- Place records in confidential folders, transport them in a secure container, and keep them under control at all times. This includes during meals or breaks.
- When working from home, keep records locked in a desk drawer or filing cabinet to reduce unauthorized viewing and access by family members or friends.

Guidelines specific to personal information stored on portable electronic devices when outside the office:

- Protect portable electronic devices containing personal information with a strong password (and preferable two-factor authentication) when taken away from the office and ensure that the storage media is encrypted.
- Avoid storing personal information on portable electronic devices unless absolutely necessary.
- To prevent loss or theft, keep portable electronic devices secure at all times in a locked briefcase, desk drawer, container, or room, and keep them under one person's control at all times. This includes during meals or breaks.
- When travelling by car, keep all portable electronic devices locked in the trunk before the start of the trip— don't put them there once at the destination. Where possible, do not leave portable electronic devices unattended, even if stored in the trunk.
- When no longer needed, remove all sensitive personal information from portable electronic devices using a digital wipe utility program. Do not rely on the delete function as the information may still remain on the device.
- All emails being sent containing patient information must be encrypted.
- Explicit written consent from the patient must be obtained before sending patient records unencrypted.

Guidelines for appropriate use of home computers/ laptops, work laptops or portable electronic devices for accessing personal information:

- Do not use public computers or networks to connect to the office network as these are not secure devices and locations.
- Do not use public Wi-Fi unless your IT professional has configured an appropriately secure VPN network tunnel.
- Log off from a laptop or home computer and set the automatic log out to occur when not in use.
- Lock home computers that are used for work-related purposes to a table or other stationary object with a security cable and keep them in a room with restricted access.
- When accessing electronic records from home, avoid storing any personal information on the hard drive of a home computer. Any personal information that must be stored on hard drives should be encrypted and password protected.
- Do not share a laptop or home computer that is used for working with sensitive personal information with other individuals, including family members and friends.
- Ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection. Ensure that the latest updates and security patches are regularly installed.
- When conducting business involving personal information over a network, use an encrypted link to the host network, such as a virtual private network (VPN).
- Ensure that staff do not remove any patient information from the office network without authorization from their supervisor.
- Watch out for "shoulder-surfing" where unauthorized individuals may casually observe the screen of someone's laptop or desk computer.
- Consider installing a privacy screen filter to prevent viewing of the screen from an angle.
- Do not extract patient information onto a portable storage device (USB) unless encrypted.
- Do not send patient information to a personal mailbox.
- Avoid using home computers entirely.