Patient records and privacy of health information practice standard

1 December 2020

Dental Council
Te Kaunihera Tiaki Niho

Foreword

Standards framework

The Dental Council (the "Council") is legally required to set standards of clinical competence, cultural competence and ethical conduct to be observed by all registered oral health practitioners ("practitioners")[a]. This means that compliance to the Council's standards by practitioners is mandatory.

The Council has established a standards framework which defines the ethical principles, professional standards and practice standards that all practitioners must meet.

There are five ethical principles that practitioners must adhere to at all times.

Practitioners must:

- put patients' interests first
- ensure safe practice
- communicate effectively
- provide good care
- maintain public trust and confidence.

Each of the five ethical principles is supported by a number of professional standards which articulate what a practitioner must do to ensure they achieve the ethical principles. The professional standards are, in turn, supported by practice standards which relate to specific areas of practice that require more detailed standards to enable practitioners to meet the professional standards and ethical principles.

A copy of the standards framework is available on the Council's website.

Compliance

The standards set by the Council are minimum standards which are used by the Council, the public of New Zealand, competence review committees, professional conduct committees, the Health and Disability Commissioner, the Health Practitioners Disciplinary Tribunal and the courts, to measure the competence, performance and conduct of practitioners.

A failure to meet the Council's standards and adhere to the ethical principles could result in Council involvement and may impact on the practitioner's practice.

Sometimes factors outside of a practitioner's control may affect whether or not, or how, they can meet the standards. In such circumstances, practitioners are expected to adhere to the ethical principles, demonstrate insight and use their professional judgement to determine appropriate behaviour.

Practitioners must be able to justify their behaviour when this is contrary to the standards, and document their reasons.

[a] Oral health practitioners include dentists, dental specialists, dental hygienists, dental therapists, oral health therapists, clinical dental technicians, dental technicians, and orthodontic auxiliaries.

Contents

Introduction

This introduction provides commentary on the patient records and privacy of health information practice standard and context for the standards and guidance within it. It does not form part of the practice standard.

The patient records and privacy of health information practice standard contains:

- The Dental Council *standards* (the 'standards') for patient records and privacy of health information that all registered oral health practitioners ('practitioners') **must** meet. These are presented in the numbered coloured boxes -

#	The standards that practitioners must meet.

  and

- *Guidance* which describes the actions and behaviour that enable practitioners to meet the minimum standards. If a practitioner does not follow the guidance, they must be able to demonstrate to the Dental Council (the 'Council') that they meet the standards.

  This is presented in the grey-shaded boxes directly following the relevant standard -

Guidance
➢ The actions and behaviour that enable practitioners to meet the minimum standards.

In this practice standard the guidance also contains some explanatory notes to assist practitioners' understanding of the standards.

Purpose

The purpose of the patient records and privacy of health information practice standard is to set minimum standards for oral health practitioners in creating and maintaining patient records and maintaining the privacy of patients' health information.

Patient records assist practitioners in providing safe, effective, and complete care—and enable them to collaborate effectively with their colleagues and other health practitioners, in the interests of good patient care. They may also be used in forensic investigations and complaint resolution, and in quality review and audit processes.

The standards apply to patient records and health information regardless of the form in which it is held, or where, and covers paper-based and digital records.

Duty of patient care

In accordance with the standards framework, practitioners have a responsibility to ensure safe practice and put their patients' interests first by maintaining accurate, time-bound and up-to-date patient records and protecting the confidentiality of patients' health information.

Patient health information is collected within the context of the practitioner-patient relationship—a partnership based on trust and respect which is focused on meeting the oral health needs and goals of the patient. It is vital that practitioners maintain patient trust by treating all patient health information as sensitive and confidential.

The Code of Health and Disability Services Consumers' Rights provides that every consumer has the right to have services provided with reasonable care and skill[1] that comply with legal, professional, ethical and other relevant standards[2]; this includes treating patient information appropriately.

New Zealand law and standards

The Privacy Act 2020 applies to any action taken and all personal information collected or held by a New Zealand entity, both inside and outside New Zealand; and to any action and all personal information collected or held by an overseas entity in the course of "carrying on business" in New Zealand.[3]

Where the information concerns a patient's health, the Health Information Privacy Code 2020 ('HIPC') additionally applies, and has the same legal standing as the Privacy Act. Where the HIPC is mentioned in this document, the reference may also be to relevant parts of the Privacy Act.

The HIPC defines 'health information' in relation to an identifiable individual as:

(a) Information about the health of that individual, including that individual's medical history

(b) Information about any disabilities that individual has, or had.

(c) Information about any health or disability services that are being provided, or have been provided, to that individual.

(d) Information provided by that individual in connection with the donation, testing, or examination, of any body part or bodily substance, of that individual.

(e) Information about that individual which is collected prior to, or in the course of, and incidental to, the provision of any heath or disability service to that individual.

Typically, in the dental context, patient health information is contained in the patient record, which also includes financial transactions associated with services that have been provided.

The *New Zealand Standard Health Records* (NZS 8153:2002) sets out the minimum requirements for the appropriate documentation and management of health records within public and private healthcare services in New Zealand.

The standards and guidance in the practice standard are principally based on the legal and professional obligations described in the Privacy Act and the HIPC, the Health (Retention of Health Information) Regulations 1996 and the NZS 8153:2002.

Standards 3- 15 are linked in order to the rules of the HIPC, and the guidance reflects elements of the HIPC's commentary thought to be the most relevant to dental practice. However, this practice standard is not intended as a substitute for the HIPC, and it is recommended that the HIPC be read in conjunction with the practice standard.

On the record. A practical guide to health information privacy, published by the Office of the Privacy Commissioner, may be a useful additional reference in this practice area.

[1] Right 4(1) Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
[2] Right 4(2) Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
[3] Section 4 of the Privacy Act 2020

Components of the patient record

The patient record includes (but is not limited to):

- Completed patient questionnaires—including patient information required for administrative purposes, and medical and dental history
- Radiographic images, clinical photographs, and models
- Clinical notes documenting assessments, diagnosis, recommendations for prevention of disease and promotion of oral health, and treatment offered and provided, or declined
- Information and documents related to informed consent
- Results or reports related to special tests or investigations
- Digital information related to computer assisted restoration design and construction processes
- Correspondence (or copies of) related to the patient
- Financial transactions.

Ownership of patient records

While physical patient records (forms, computer systems etc.) are owned by the dental practice owner(s), patients are entitled to access and seek correction of their health information, and may request their original records which may be transferred to them, subject to a small number of specific grounds for refusal.[4] Patients do not have the right to take away original records (see standards 8 and 9).

Responsibilities for staff

The HIPC holds a 'health agency' responsible for the actions of those working for it, whether paid or unpaid, except where the person was clearly working outside his or her authority or instructions. The term 'health agency' covers all providers of public or private health or disability services[5], dental practices included.

Therefore, dental practice owners are responsible for ensuring that staff understand and comply with the legal obligations of the HIPC, reflected in the standards and guidance of this practice standard. It is anticipated that staff briefing, or training would be necessary to enable staff to properly manage patient records and maintain the privacy of patient information.

[4] Found in sections 49 - 53 of the Privacy Act 2020
[5] Health Information Privacy Code 2020

Role of the privacy officer

Section 201 of the Privacy Act requires a health agency to have at least one person acting as a "privacy officer"—whose responsibilities include:

- Encouraging the agency to comply with the information privacy principles in the Privacy Act and rules in the HIPC
- Dealing with requests made to the agency under the Privacy Act and HIPC
- Working with the Privacy Commissioner in relation to any investigations conducted under the Privacy Act in relation to that agency
- Ensuring compliance by the health agency with the Privacy Act and the HIPC.

The person does not have to be dedicated only to information privacy issues. However, the responsibilities listed above do need to be included in the duties of at least one person within the dental practice.

The Privacy Act also requires all health agencies to have procedures to enable appropriate and timely management of complaints, and to designate a person to deal with complaints related to privacy issues. This person may be the privacy officer or another individual within the dental practice.

Patients are entitled to know of their right to complain directly to the Privacy Commissioner when they feel their privacy has been infringed.

Acknowledgements

The Patient records and privacy of health information practice standard is founded on a number of different sources, including the *Health Information Privacy Code (HIPC)2020*, the *New Zealand Standard Health Records* (NZS 8153:2002), the *Health (Retention of Health Information) Regulations* 1996**,** *the Health Act 1956,* the Privacy Commissioner's publication *On the record: a practical guide to health information privacy,* and the New Zealand Dental Association's code of practice *Patient information, privacy and records.*

This page is intentionally left blank.

Patient records and privacy of health information practice standard

Dental Council
Te Kaunihera Tiaki Niho

Creating and maintaining patient records

1 You must create and maintain patient records that are comprehensive, time-bound and up to date; and that represent an accurate and complete record of the care you have provided.

Guidance

- Understand that the patient, or an authorised third party, may read the information in the patient record you create.
- Use language that is professional and objective, and that accurately represents the care provided including any relevant discussions and interactions between the patient and yourself.
- Write clearly and only use standard abbreviations and acronyms, so the information can be easily understood by the patient or authorised third parties who may access the record.
- Enter information in the patient record as soon as practical after providing care, make sure all entries are dated, and keep entries in chronological order. Ensure computerised entries are time logged.
- Make sure the entries you make can be recognised as being made by you. You are responsible for entries related to patient care you provide.
- For written records—write legibly using an indelible pen.
- Check the accuracy of information that is subject to change over time, and update this information at appropriate intervals to make sure the patient record is kept up to date. For example, contact details, medical history.
- Record the following information in the patient record:
    - The name, gender, date of birth, contact details of the patient
    - If the patient is under 16 years of age, or does not have legal capacity – the contact details of the patient's representative (see HIPC definition of representative in this context, provided as Appendix A)
    - A concise and relevant signed medical history which is updated at appropriate intervals
    - The date and details of any patient contacts, for example, appointments, telephone calls; and any appointment the patient has failed to attend.
    - Reason for attendance, including details of any presenting complaint
    - Relevant history, clinical observations and findings, and diagnosis
    - Treatment options given, information given to the patient on associated benefits, likely outcomes of care, and potential risks, and final care plan for which consent is obtained.
    - A record of any proposed care that is declined by the patient, along with the patient's related comments or concerns.

- A concise description of care provided, including:
    - recommendations given for prevention of disease and promotion of oral health
    - any medicines administered, prescribed, or dispensed including the quantity, dose and instructions (including local anaesthetic)
    - general comments on the procedures performed
    - variation from any standard or usual technique
    - materials used
    - batch control identification (BCI) information, when relevant
    - pre- and post- operative instructions given to the patient.
- Unusual responses to care provided, including adverse drug reactions which may be reported by the patient. Inform Medsafe of any adverse drug reactions and note that you have done this in the patient's record.
- Estimates or quotes for fees involved and any arrangements for payment.
- Any complaints made, or concerns expressed, regarding the care provided.

➢ In addition to the above recorded information, the patient record includes (but is not limited to) the following:

- Completed patient questionnaires - including patient information required for administrative purposes, and medical and dental history
- Radiographic images, clinical photographs, and models
- Information and documents related to informed consent
- Results or reports related to special tests or investigations
- Digital information related to patient care, for example, computer assisted restoration design and construction processes
- Correspondence related to the patient, for example referral letters, ACC correspondence
- Financial transactions.

2 You must not delete information entered in the patient record at an earlier date, and must ensure your name and the date of entry is alongside any correction or other amendment you make.

Guidance

- For computerised records:
  - Complete a new entry if it is necessary to correct, add to, or clarify previously recorded information. Do not delete the original entry; or information contained in it.
  - Check that computerised patient records are time logged, so that any amendments to the record are dated, and that your name is recorded.
- For written records:
  - If correction of information in the patient record is necessary:
    - Draw a single line through the incorrect words, so that the original wording remains readable
    - Insert the correct words
    - Write the date the correction is made, and your name, alongside the correction.
    - Do not use correction fluid.
  - If additional information, or clarification of previously recorded information, is necessary complete a new entry and write the date and your name alongside.

Note the reason(s) for any amendment to patient information alongside the amendment made.

Collection of health information [6]

3 You must collect patients' health information only for lawful purposes connected with your professional functions and activities.

Guidance

- Be clear about why you need the information you plan to collect and how you intend to use it; and collect only information you actually need.
- Professional functions and activities may include:
  - Providing oral health care and treatment
  - Administrative aspects related to care
  - Training and education
  - Research
  - Monitoring the quality of patient care.
- Only collect a patient's identifying information when the purpose for which you are collecting a patient's health information requires it.

4 You must collect health information directly from the patient concerned where possible.

Guidance

- Collecting information from the patient concerned improves the overall quality of information, helps patients know how their information is handled, and gives them an opportunity to object if they are concerned about the proposed use of their health information.
- Collect information from a source other than the patient concerned when:
  - the patient or their representative authorises collection of information from someone else, for example, the patient's medical practitioner

[6] Standards 3 - 6 correspond to Rules 1- 4 of the Health Information Privacy Code 2020

- the collection of information from the patient could prejudice their own safety or interests, for example, when the patient has limited cognitive ability
- collection is not reasonably practical, for example, when the patient is unconscious
- the information is publicly available.

In some of these situations the person who provides the information is known as the patient's 'representative'. Appendix A provides the full definition of a 'representative', as defined in the HIPC.

➢ Be sure that someone claiming to be a patient's representative has the legal authority to do so.

➢ Record the source of information collected from anyone other than the patient concerned, and verify the accuracy of the information with the patient as soon as possible, where practical.

5

You must take reasonable steps to ensure that a patient or their representative is aware that health information is being collected, the purpose of collection, and the potential impact of not providing all of the requested information.

Guidance

➢ Reasonable steps may include:

- A verbal explanation
- A notice on display
- Explanatory notes in standard forms
- An explanatory brochure.

➢ Confirm the patient's understanding that their health information is being collected and provide a full explanation of the purpose of collection the first time information is collected.

This is not necessary on subsequent occasions, unless information sought later relates to a different purpose, for example research.

➢ Recognise and respect the patient's right not to supply any requested information.

➢ Explain to the patient the potential impact if they choose not to provide all of the requested information, for example:

- That a particular treatment cannot effectively be continued
- That a claim cannot be granted or processed.

6

You must collect health information in a manner which is lawful, and fair in the circumstances, and which does not intrude to an unreasonable extent on patients' personal affairs unnecessarily.

Guidance

- Do not mislead patients regarding the purpose of collection, provide any inducements to obtain information, or coerce health information from patients.
- Be mindful of the sensitive nature of personal information, and its importance to the patient concerned.
- Do not video or voice record patients without their consent when collecting their health information, and provide information regarding the intended use of the video or recording as part of that consent process; written consent is recommended in situations where the video or voice recording will be disclosed to others (subject to the patient authorising disclosure).

Security of health information

7 You must ensure security safeguards are in place to protect patient health information.

Guidance [7]

Physical security

➢ Protect the physical security of patient information by:

- Physically securing and restricting access to the areas in which patient information is stored. Take simple precautions such as locking filing cabinets and locking unattended rooms.
- Requiring password access to computer systems where patient information is stored and using access lockout after a fixed number of incorrect login attempts.
- Positioning computer screens so that they cannot be seen by unauthorised persons.
- Using security screen saver programmes to prevent unauthorised persons from seeing computer screens and having automatic log-off of computer systems after a set period of non-use.
- Protecting patient records from physical hazards, for example, fire.
- Backing-up patient records regularly, and testing recovery of information from the back-up.
- Storing records that are not being used for current or regular patient care, but that need to be legally held, in a manner that protects their security.

Operational security (Users)

➢ Protect the security of patient information by:

- Keeping patient information confidential—disclose health information only to the patient, or their representative, unless an exception applies (see standard 13).
- Not accessing the health information of patients, you have not provided care for, unless an exception for the use or disclosure of health information applies (see standards 10 and 13)
- Ensuring team members understand their obligations in relation to the confidentiality and privacy of patient information.
- This includes an understanding that patients' health information cannot be discussed with anyone other than team members who already hold this information, unless an exception applies. Where practical, any discussion involving patient information should occur in private areas of the practice, not in shared spaces such as the waiting room, reception area, or staff room.

[7] Standard 7 corresponds to Rule 5 of the Health Information Privacy Code 2020

- Avoiding collecting patient information verbally in public waiting areas, where discussions can be overheard
- Keeping patient information on the premises where possible and keeping information secure when there is a need for it to be off-site, for example, storing 'archived' patient records off-site.
- Anonymising patient information when being used for health education purposes and using fictitious information when training individuals in the use of systems.
- Withholding, as far as practical, access to patient information from IT services personnel.

Operational security (Computer systems)

➢ Protect the security of patient information by:

- Maintaining a list of team members who are authorised to use the system.
- Managing authorised users' access consistent with their role, so that access to patient information is on a 'need-to-know' basis.
- Using strong passwords and changing them at regular intervals.
- Making sure that computer access leaves a footprint that is regularly audited to detect unauthorised access.
- Providing training for team members on the proper use of the computer system, which includes how the security and privacy of patient information is protected.

Technical security (Computer systems)

➢ When selecting and maintaining a computer system for the collection of patient information:

- Use only software designed for recording, processing, storing, and retrieving patient information.
- Set up security, firewalls, and anti-malware systems to protect patient information from direct unauthorised access, and unauthorised access through hacking or invasion of hostile or intrusive software.
- Use a back-up system which allows information to be stored remotely from the main computer system, preferably off-site.

➢ If you are using remote servers hosted on the internet to manage and/or store patient information (also termed 'cloud computing'), you remain responsible for the security of that information.[8]

The same applies if you are using a third party for storage of patient information in digital form where the remote server is not internet based.

Make sure that when using these services patient information is sent and stored safely by being assured:

- that the data is automatically encrypted when it is being sent between your practice and the remote server
- of the physical and digital security of the remote sever.

[8] Transfer of information to an offshore data processor (eg a cloud storage provider) will (usually) not constitute an overseas disclosure for the purposes of Rule 12 of the Health Information Privacy Code 2020

The Privacy Commissioner has further detailed guidance in this area, and may be useful resources for practitioners.

Security of transmission

- Consider developing a practice procedure for sending out patient health information that reflects the guidance below:

For email	• Consider the nature of the information to be sent, who the intended recipient is, and whether email is the most appropriate form of communication. If the email recipient is a patient, confirm that you have their permission to communicate with them in this way. • When sending sensitive information, encrypt email contents (both user and recipient will need to use the same encryption), or use password protection. • Ensure email addresses are accurate and current. • Consider using a secure email service. • Do not use lengthy 'chains' of responses in emails, as sensitive information may be unwittingly included by an earlier response. • Limit the number of "cc" addresses to only those who must receive the information.
For post	• Ensure the type of physical delivery is appropriate for the nature of the information (general post, registered post, couriered post, track-and-trace, and hand delivered post). • Ensure addresses are accurate and current. • Ensure postal items are kept secure until lodged.
For text messaging	• Check you have the patient's consent to send them text messages, for example, appointment reminders; and record their consent or refusal in the patient record. • Do not include clinical information in text messages.
For facsimile (Fax)	• Limit the use of fax machines to authorised persons and control the type of information that may be sent. • Programme fax machines with frequently called numbers to reduce the risk of misdialing (regularly check the accuracy of these). • Check that correct transmission has occurred, and respond rapidly in the case of incorrect transmission.

- Do not give patient records to third parties, such as the patient's relatives or friends, to hand deliver to a patient, unless authorised by the patient concerned, or the person is the patient's representative.

Security during destruction

- Destroy physical records by controlled incineration or shredding, ensuring that no information is lost or removed during the process and that the resulting waste does not include fragments of readable personal information. Alternatively, a reputable document destruction company can be used.

- Destroy computerised records by using an appropriate electronic or physical process to ensure the record is unreadable. Simple deletion from the device may be inadequate as data recovery is possible. Seek expert advice if you are unsure.

Security breaches

- Act promptly to manage an actual or suspected breach of patient information.

- Appendix B outlines the mandatory reporting requirements under the Privacy Act 2020, and key steps that the Privacy Commissioner says should be followed, and be incorporated into a practice procedure which specifies how to deal with information breaches.

Patients' access to their health information

8 You must give patients access to their personal health information on request, and in the form the patient prefers when possible—except when withholding grounds contained in the Privacy Act 2020 apply.

Guidance [9]

- Patients are entitled to receive confirmation whether you hold health information about them.
- Patients are entitled to access their health information. Respond to a patient's request for access to their health information as quickly as possible, and within 20 working days after the request is made.[10]
- If the patient is given access to their health information, they must be advised that they may request the correction of that information.
- Inform the patient of any delay in retrieving their information, the reasons for the delay, and when they can expect to receive their information.
- Inform the patient if you refuse them access to their information and explain why. Grounds for withholding patient information are limited, and can be found in sections 49, 50, 51, 52 and 53 of the Privacy Act 2020. Some of the more common reasons for refusing access may include:
  - When the information is not readily retrievable—if refusing access on these grounds you need to demonstrate that a reasonable effort has been made to retrieve the record.
  - When the information does not exist or cannot be found—it is advisable to confirm with the patient exactly what information is being sought before refusing on these grounds.
  - When the record contains information about another individual—the requested information can be made available with appropriate deletions and/or alterations protecting this information, and reasons for withholding certain information provided.
  - When the patient is under 16 years of age, and disclosure of that information would be contrary to the patient's best interests.
  - When information about the patient is 'evaluative material' (as defined in section 50 of the Privacy Act 2020), and has been supplied by another person in confidence, and disclosure to the patient would breach a promise made to that person that the information and/or their identity would be held in confidence.
  - When disclosure would be likely to create a serious threat to the health, safety, or life of an individual, or to public health or safety.
  - When disclosure would create a significant likelihood of serious harassment to an individual or cause significant distress to a victim of an offence.

Access cannot be refused on the basis of money owed, or that the practitioner 'owns' the records.

[9] Standard 8 corresponds to Rule 6 of the Health Information Privacy Code 2020
[10] Section 44 of the Privacy Act 2020

- When a request for access is made either orally or in writing:

    - Be satisfied as to the identity of the individual making the request. Parents or guardians may make requests on a child's behalf but only in the child's interest, not their own.

    - Make sure the information is received only by that patient or their representative; and that any representative is authorised to obtain the information. This may involve having the patient or representative sign a receipt for the information—to be kept for record purposes.

- Provide information in the form requested unless it would be problematic or very expensive, be contrary to any legal duty, or grounds for withholding the information apply.

  Patient information may be made available in a variety of forms including: inspection of documents, providing a printed or electronic copy of the documents, viewing radiographs, supplying a written summary, or a verbal explanation.

  Patients may request their original records, and you may transfer their records to them. However, patients do not have the right to take away original records.

- Do not ask patients to pay for access to their health information. You may ask for a reasonable fee, (for example, administrative expenses incurred), if a patient makes a request for the same or substantially the same health information more than once within a period of twelve months, for the second or subsequent requests.

  You may ask for a reasonable fee, based on actual costs, for the duplication of non-digital radiographs, photographs, or study models. Where this exceeds $30, you must provide the patient with an estimate of the charge before dealing with the request.[11]

[11] Part 3 (6) of the Health Information Privacy Code 2020

Correction of health information

9 You must take reasonable steps to correct patients' health information, on their request.

Guidance [12]

- Consider a patient's request that their health information be corrected. If you decline the request, provide the patient with the reasons why. Reasons for refusal to correct information may include, but are not limited to, the following:
  - You believe the original information is correct
  - The information identified for correction is clearly identifiable as opinion, and correctly represents the opinion held at the time
  - You believe the information to be correct at the time it was recorded, circumstances have changed and there are no means of verifying correctness.
- Note in the patient record that a correction to their health information was requested by the patient.

  If you decline to make a correction, note the reason why and attach any statement provided by the patient setting out what they wanted the correction to be in the file.

  When you make a correction, follow the guidance for Standard 2.
- Do not request payment for requests for correction of the record or attaching additional information to the record.

[12] Standard 9 corresponds to Rule 7 of the Health Information Privacy Code 2020

Checking accuracy of health information before use or disclosure

10 You must check that health information that is collected and recorded by someone else is accurate, up-to-date, and complete before using or disclosing it.

Guidance [13]

- There will be situations where you receive patients' health information that has been collected and recorded by someone else, for example, another practitioner or staff member (depending on the nature of the information).

  Consider the following when determining what steps you need to take to check this information before using or disclosing it:

  - The proposed use
  - The age of the information and the reliability of its source
  - The practicalities of verifying accuracy or currency
  - The probability, severity, and extent of potential harm for the patient if the information is inaccurate.

  Generally, the more important the information is to its proposed use, the more rigorous the steps you take to ensure its accuracy and completeness. The first source for checking of information is the patient.

[13] Standard 10 corresponds to Rule 8 of the Health Information Privacy Code 2020

Retention of patient records

11

You must ensure that your patients' records are retained for a minimum of 10 years from the day following the last date on which care was provided, or the records are properly transferred. [14]

Note: Under the Public Records Act 2005 patient records held by DHBs are considered public records, and may not be disposed of without the authorisation of the Chief Archivist.

Guidance [15]

- You may retain patient records for longer than 10 years from the day following the last date on which care was provided to the patient if it is anticipated that they might be needed for future diagnosis and care, and are kept securely.
- Patient records do not need to be retained in any particular form. Electronic copies of records may be made as long as the information is reproduced accurately and is accessible.
- You may, within the 10-year period described above, transfer original patient records to the patient, their representative, or another practitioner or dental practice. Typically, this would be on the patient's request.

  Once you transfer the complete, original record to the patient or their representative, you no longer have any obligations related to the retention of that record. This is also the case if the record is transferred to another practitioner or dental practice—the practitioner or dental practice receiving the record now has these obligations.
- If you transfer the original record, it is recommended that you retain a copy of the record for situations such as a future complaint regarding the quality of care provided, or financial auditing purposes.
- Arrange the transfer of patient records before retiring. This will involve informing patients of your plans for the transfer of their health information to another practitioner on the sale or closure of your practice. This provides the opportunity for the patient to request that their personal information is instead transferred to them, an alternative dental practice or practitioner.

[14] This is a requirement of the Health (Retention of Health Information) Regulations 1996
[15] Standard 11 corresponds to Rule 9 of the Health Information Privacy Code 2020

Limits on use of health information

12 You must only use health information for the purpose for which it was collected unless the patient gives their permission for it to be used for another purpose, or another exception of the HIPC applies.

Guidance [16]

- Exceptions that allow for health information to be used for a purpose other than that for which it was collected, without the patient's permission, include:
  - When the information is used for a directly related purpose, for example, administrative uses
  - When the origin of the information is from a publicly available source, for example, the register of births, deaths and marriages, telephone directory, publicly available websites, or other internet sources
  - When its use is necessary to prevent or lessen a serious threat to public health or public safety, or somebody's life or health. When deciding if a threat is serious, consider its imminence, likelihood, and potential severity.
  - When the information is used in a form that does not identify the patient, that is, information identifying the patient has been removed (peer group discussions, case study reports).
  - When the information is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the patient concerned—noting that in most instances approval from an ethics committee will first be needed.
  - When the information is necessary to avoid prejudice in the maintenance of the law; or for court proceedings that have commenced or are reasonably in contemplation.
- Where practical, it is recommended that you ask for the patient's permission when you want to use their health information for another purpose, and in particular for research and formal education purposes.

[16] Standard 12 corresponds to Rule 10 of the Health Information Privacy Code 2020

Limits on disclosure of health information

13 You must disclose health information only to the patient concerned, or their representative[17] unless the patient or their representative authorises the disclosure, or another exception of the HIPC applies.

Guidance [18]

- Other noteworthy exceptions of the HIPC that allow for disclosure of patient information are listed in the guidance of Standard 10, with one additional exception—that the disclosure is for the same purpose for which the information was obtained, for example for further treatment of the patient by another practitioner.

  This is consistent with the Health Act 1956 which allows for the disclosure of patient information to another practitioner on their request, in order for them to provide health or disability services to the patient. In most circumstances you are obliged to provide this information. However, if you believe the patient concerned would not want the information disclosed to the requester, you may refuse.

- Other legislation allows for the disclosure of information to various agencies if that information is required for those people to carry out their functions, for example, dental records may be requested by the police to assist in identification.

  When the basis for such a request is unfamiliar, request in writing exactly what information is required and the statutory provision which requires you to provide it, before disclosure.

- In most circumstances when an exception applies, the decision whether or not to disclose information remains at your discretion. Consider your professional and ethical obligations in making your decision.

- Disclose information only to the extent necessary to meet the purpose or request when you do not have the authorisation of the patient concerned, or their representative.

- Disclose information to a relevant authority or person in cases of suspected neglect or abuse of a child or young person. The Oranga Tamariki Act 1989 has provisions which allow this disclosure.[19] When considering disclosing information under the information sharing provisions in sections 66 – 66Q of the Oranga Tamariki Act 1989, you must have regard to the principle that the well-being and best interests of a child/young person, in general, take precedence over your duty of confidentiality to the child/young person or any other person. While disclosure is not mandatory, it is considered an ethical and professional obligation.

- If approached by a researcher seeking the disclosure of health information, be sure that ethical approval has been obtained, and that information will not be published in any form that could identify the patient(s). If health information is to be disclosed and used for research purposes, ask the patient(s) for authorisation, unless this is not practical.

[17] Appendix A provides the full definition of 'representative', as defined in the Health Information Privacy Code 2020
[18] Standard 13 corresponds to Rule 11 of the Health Information Privacy Code 2020
[19] Sections 15, and 66 - 66Q

Disclosure of health information outside of New Zealand

14 You must only disclose health information outside of New Zealand if you have taken reasonable steps to ensure the information is protected by acceptable privacy standards.

Guidance [20]

- This Rule in the HIPC does not apply where you are simply using an overseas agency to hold, process or store health information on your behalf as your 'agent' and the other agency is not using the information at all. This is not treated as a disclosure under the Privacy Act.

  For example, when an overseas company provides cloud-based IT services for a New Zealand organisation. In this case you will be responsible for ensuring that your 'agent' – the overseas company – handles the information in compliance with the requirements of the Health Information Privacy Code 2020 (HIPC) and Privacy Act 2020.

- Only disclose health information to an agency outside New Zealand if the receiving agency:

  - is carrying on business in New Zealand and, in relation to the information disclosed you believe on reasonable grounds that the agency is subject to the Privacy Act, as modified by the HIPC; or
  - is subject to privacy laws that provide comparable safeguards to the Privacy Act, as modified by the Health Information Privacy Code 2020; or agrees to be subject to contractual information protection obligations comparable to the protections to the Privacy Act, as modified by in the HIPC; or
  - is covered by a binding scheme specified in regulations made under section 213 of the Privacy Act 2020 or is subject to the privacy laws of a prescribed country specified in regulations made under section 214 of the Privacy Act 2020; or
  - the individual concerned, or that individual's representative where the individual is dead, or is unable to exercise their rights under these rules, authorises the disclosure (after being informed that the destination where their information will be held does not have comparable protections to those in the Privacy Act, as modified by the HIPC).

  The Office of the Privacy Commissioner has developed model contractual clauses that are available on the Privacy Commissioner's website.

- You may disclose health information to an overseas agency where it would not otherwise be allowed if the disclosure is necessary to maintain public health or safety, to prevent a serious threat to someone's life or health, or for the maintenance of the law.

[20] Standard 13 corresponds to Rule 12 of the Health Information Privacy Code 2020

Unique identifiers

15 You must use unique identifiers only for the purpose of enhancing practice efficiency; and must not use the same identifier given by another body, with the exception of the patient's NHI number.

Guidance [21]

- Unique identifiers are numbers, letters, or combinations of these, designed to identify the patient record without the use of the patient's name.
- Consider whether using unique identifiers will increase the efficiency of the functions being carried out in delivering patient care—if not, then avoid their use.
- If you do use them, do not use the same identifier given by another body, for example licence or passport numbers. The patient's National Health Index (NHI) number is the exception to this rule, it may be used by multiple health agencies.
- You must take steps that are reasonable in the circumstances to ensure that the risk of misuse of a unique identifier is minimised. For example, this might include checking the person's identity (ie by checking their date of birth and full name etc.) where the person is not known to the practitioner before using the NHI number associated with the person.

[21] Standard 14 corresponds to Rule 13 of the Health Information Privacy Code 2020

Appendices

Dental Council
Te Kaunihera Tiaki Niho

Appendix A: HIPC definition of ‘representative’

Representative, in relation to an individual, means:

- Where the individual is dead, that individual’s personal representative (for example, the executor, or administrator of the estate); or
- Where the individual is under the age of 16 years, that individual’s parent or guardian; or
- Where the individual, not being an individual referred to in paragraphs (a) or (b), is unable to give his or her consent or authority, or exercise his or her rights, a person appearing to be lawfully acting on the individual’s behalf or in his or her interests.

Appendix B: Key steps in the management of a privacy breach[22]

Privacy breach

A health information privacy breach in relation to health information held by an agency occurs when there is: [23]

(a) Unauthorised access to, or disclosure, alteration, loss or destruction of, the health information; or

(b) An action that prevents the agency from accessing the information on either a temporary or permanent basis; **and**

includes any of these actions or things listed in (a) or (b) above whether or not the action or thing:

(a) was caused by a person inside or outside the agency; or

(b) is attributable in whole or in part to any action by the agency; or

(c) is ongoing.

Privacy beaches often involve people's health information being accidentally lost or disclosed, for example, being emailed to the wrong person or a breach in system security.

Notifiable privacy breach

A notifiable privacy breach means a privacy breach that it is **reasonable to believe has caused serious harm** to an affected individual or individuals **or is likely to do so.** When assessing whether a privacy breach is likely to cause serious harm you must consider the factors set out at section 113 of the Privacy Act.

The Privacy Commissioner has an online tool **NotifyUs** that is available to assist agencies in determining if a breach is notifiable and to guide agencies through the notification process. The Privacy Commissioner expects that agencies will use this tool.

If a privacy breach **that meets the definition of a notifiable privacy breach in the Privacy Act 2020)** occurs, you must:

- Report the breach to the Privacy Commissioner as soon as possible;[24]
- Report the breach to the person/people concerned as soon as possible **unless** an exception in the Privacy Act 2020 applies;[25]

Individuals must be notified directly, or through a public notice if it is not reasonably practicable to notify an affected individual or each member of a group. Notification to an individual or group must cover the prescribed list of information set out at section 117 of the Privacy Act 2020.

You may be able to delay notifying affected individuals, or to give a public notice of a notifiable privacy breach if one of the exceptions in section 116 of the Privacy Act 2020 applies. However, if you rely on this exception in the Privacy Act, you must notify affected individuals once the grounds for delay no longer exist, or no longer outweigh the benefits of informing affected individuals.

[22] Adapted from the Privacy Act 2020 and the Health Information Privacy Code 2020
[23] Section 112 of the Privacy Act 202
[24] Section 114 of the Privacy Act 2020
[25] Sections 115 and 116 of the Privacy Act 2020

There may also be contractual and professional obligations to report the breach to other parties (e.g. contracts with DHBs and ACC).

You should also do what you reasonably can to minimise the harm to both the people affected and the organisation.

Key steps to managing a privacy breach

The steps set out below and in guidance published by the Privacy Commissioner apply to all incidents of a privacy breach, or suspected privacy breach, whether the breach reaches the threshold of a notifiable privacy breach or not, and should be followed.

These steps may be included in a practice procedure which specifies how to deal with privacy breaches.

Contain the breach and carry out a preliminary assessment

- Take immediate steps to contain the breach and stop further loss or disclosure of health information. Appoint a suitable person to investigate the breach (this may be the privacy officer)
- Determine whether the breach reaches the threshold for a **notifiable privacy breach** (i.e. there is reason to believe the breach has, or is likely to, cause **serious harm** to an affected individual(s)) by using the available on the Office of the Privacy Commission website.
- When using NotifyUs you will consider the factors set out in section 113 of the Privacy Act 2020:
  - Any actions taken by the agency to reduce the risk of harm following the breach
  - The sensitivity of the health information involved in the breach
  - The nature of the harm that may be caused to affected individuals
  - The person or body that has obtained or may obtain the health information as a result of the breach (if known)
  - Whether the health information is protected by a security measure (such as encryption or anonymisation)
  - Any other relevant matters.

If the breach reaches the threshold of a 'notifiable privacy breach'

- Notify the Privacy Commissioner of the breach as soon as possible.
- Notify the affected individual(s) as soon as possible **unless** an exception in section 116 of the Privacy Act 2020 applies.
- If it is not practicable to notify each individual concerned give a public notice of the breach **unless** an exception in section 116(4) of the Privacy Act 2020 applies.
- Consider who else urgently needs to know of the breach, both internal and external to the practice, for example, the principal practitioner or practice owner, other agencies such as ACC, Ministry of Health.
- Ensure the notification(s) include all the information required under section 117 of the Privacy Act 2020.
- Follow the guidance for managing a notifiable privacy breach published by the Privacy Commissioner on their website.

Where the privacy breach does not meet the threshold for a notifiable breach

- Notify those affected by the breach in circumstances where not notifying them would carry particular risks, even though you do not believe the risks reach the threshold of 'serious harm'.
- When notifying of the breach:
  - provide information about the incident and its timing, as well as a description of the health information involved in the breach and what you have done to control or reduce the harm
  - consider whether it is appropriate to notify any external bodies, such as insurers, professional bodies, ACC, and the Office of the Privacy Commissioner (even though this is not a notifiable breach)

Following all privacy breaches

- Consider using the outcome of the investigation to improve procedures and prevent future breaches – particularly if the breach is systemic rather than an isolated occurrence.
- A physical and technical security audit, and a review of staff training, and procedures may be productive.

Further detailed guidance on dealing with a breach is available from the Privacy Commissioner's website.