Victoria Clinic
Urgent Care Standard 2015- Indicator 1.2.1
Privacy Policy
RNZCUC & RNZCGP

1. Policy Statement

Victoria Clinic is committed to collecting, storing and using information in accordance with the Privacy Act 2020, the Health Information Privacy Code 1994 and the Employment Relations Act 2000 and subsequent amendments.

2. Policy Objective

2.1. To ensure staff are aware of their legislative obligations relevant to privacy of information.

3. Authorisation

The Directors and Practice Manager have delegated authority to approve this policy.

This policy applies to all staff at Victoria Clinic including locums and contractors.

This policy will be reviewed every two years and updated if any changes are required.

4. Definitions

4.1. **The Privacy Act 2020 effective 1 December 2020:** An Act passed to promote and protect the privacy of information collected from and about an individual.

4.2. **Code of Practice:** A Code established by the Commissioner under section 32.

4.3. **Commissioner** means the Privacy Commissioner holding office under the Crown Entities Act 2004

4.4. **Personal Information** means information about an identifiable individual; and Includes information relating to the death that is maintained by the Registrar-General

4.3. **Privacy officer:** Appointed by each practice to meet the requirements of the Privacy Act, the Privacy officer is responsible for:

4.3.1. Ensuring that the practice complies with the Privacy Act in relation to staff, and the Health Information Privacy Code in relation to patients
4.3.2. Dealing with requests made to the practice about personal or employment information
4.3.3. Working with the Privacy Commissioner or investigating officer should the need arise.

5. References and relevant legislation (this list is not exclusive)

5.1. Privacy Act 2020
5.2. Health Information Privacy Code 1994
5.3. Enrolment Requirements for Primary Health Organisations 2011
Notifiable breach: In accordance with the Privacy Act 2020 effective 1 December 2020 a notifiable breach can be reported either by e-mail, phone or by using the **online** form on https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/
5.4. **Tool to assess whether a breach must be notified**: https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/evaluate
5.7 **Reporting Requirements**: https://privacy.org.nz/assets/DOCUMENTS/NotifyUs-Reporting-Requirements.pdf

6. Related policies and procedures

6.1. Complaints policy

6.2. Incident management policy

6.3. Code of Health & Disability Services Consumers' Rights policy

7. Processes

7.1. All staff will understand, comply with and implement the practice privacy policy.

7.2. The appointed Privacy Officer for Victoria Clinic is Practice Manager. This person is responsible for monitoring privacy issues and acting on feedback from patients and staff.

7.3. Guidance in managing privacy issues is available directly from the Office of the Privacy Commissioner – telephone 0800 803 909.

8. Procedures Regarding Patient Information

8.1. Collection of Patient Information

8.1.1. Any information collected will be related to:
- the patient's care and treatment
- administrative purposes such as billing and claims management
- monitoring quality of patient care, treatment and health status such as audit

8.1.2. Information will be collected from the individual concerned in the first instance except where:
- the patient has authorised the information to be collected from someone else
- where the collection of information from the patient is not reasonably practical
- where the collection of information from the patient would prejudice their interests, the purpose of collection or the safety of any person

8.1.3. When collecting information staff will inform patients verbally by way of explanation and visually via practice posters and letter to new patients:
- that the information is being collected
- why the information is being collected
- who will receive the information
- any consequences if the information is not provided
- their rights to the information and correction

8.1.4. When collecting information verbally (in person, or over the telephone) staff must ensure the conversation cannot be overheard by unauthorised persons.

8.1.5. Ensure any patient information that is transmitted electronically is protected i.e. email, text. Where possible remove any identifying information.

8.1.6. Be sensitive about who collects the information and how it is collected.

8.1.7. Collect only information which is necessary for the purposes for which it is intended.

8.1.8. We may collect information about you from other sources, if we collect information about you indirectly and you have not already been informed that this may occur, we will, where practicable, notify you. This may be done through the portal or other appropriate means.

8.2. **Disclosure of information to a patient**

8.2.1. Rule 6 of the Health Information Privacy Code gives patients or their authorised agent the right to access information about themselves.

8.2.2. Any requests by a patient to access information held about them will be directed to the Privacy officer who will proceed as follows:

a) Contact the patient requesting access and determine the legitimacy of the request.
b) Where deemed necessary, the person will be asked to provide proof of identity. A copy of proof of identification will be scanned to the patient's file with the request.
c) Agree a timeframe within which a decision on providing access to the information will be made. This must be as soon as practicable and no later than 20 working days after the request was made.
d) Advise the patient's general practitioner of the request.
e) In consultation with the general practitioner, establish if there is any ground on which to withhold any information and if so, take appropriate action.
f) Contact the patient and agree when, where and in what format information will be provided. Where possible this should be in the format preferred by the patient and may include:

- Inspection of the documents
- Providing a copy of the document. ***N.B.*** *Patients are not entitled to demand original documents*
- Hearing or viewing audio or video tapes
- Supplying transcripts
- Supplying a summary of information
- Orally

8.2.3. Information may not be withheld, nor any charge made, on the grounds that the patient has an outstanding account with the practice.

8.3. **Disclosure of patient information to a third party**

8.3.1. Managing requests for disclosure of information by a third party is addressed in Rule 11 of the Health Privacy Information Code.

8.3.2. All such requests will be directed to the Privacy officer.

8.3.3. The Privacy officer will establish if statutory provisions require the information to be disclosed. Examples of this include, but are not limited to:

- Land Transport Act 1998, ss 18 and 19 requiring disclosure relating to driving
- Cancer Registry Act 1993, ss5,6 and 7 requiring disclosure of a diagnosis of cancer
- Tuberculosis Act 1948, s3
- Mental Health Act 1992, s22
- Health and Disability Commissioner Act 1994, s62
- Privacy Act 1993, s91

8.3.4. Where disclosure is not required, the Privacy officer will consult the patient's general practitioner and decide whether disclosure is permissible under the legislation and if it is ethically appropriate. External advice will be sought as required to assist in reaching a decision and planning a response.

8.4. **Mandatory breach notification**

8.4.1 If a privacy breach is identified and it is reasonably believed to have caused (or is likely to cause) serious harm, the Office of the Privacy Commissioner (OPC) and affected individuals must be notified as soon as practicable.

8.4.2 The liability for the breach notifications sits with Victoria Clinic and not the individual employee.

8.4.3 **Serious harm**: Consider the sensitivity of the information lost, actions taken to reduce the risk of harm, the nature of the harm that could arise, and any other relevant information. A breach that does not meet the serious harm threshold does not have to be reported to the OPC.

8.5 Requests for transfer of patient records

8.5.1 Patients' records will be transferred to other providers on receipt of a written request. The request must include the written or documented verbal consent of the patient.

8.5.2 Requests for the transfer of notes will be forwarded to the Privacy Officer or delegated personnel who will:

a. Determine that the request is appropriately documented.
b. Advise the patient's general practitioner of the request.
c. Organise the transfer, ensuring copies of all notes are retained.
d. File a copy of the request by scanning the request to the patient's PMS file.
e. Ensure the transfer is completed within 10 working days of receipt of the request.

8.5.3 Patients transferring into this practice will be asked to complete a form requesting their notes be transferred in. General practitioners will be responsible for ensuring the patient understands that the purpose of this is to facilitate the provision of effective primary care, and provide the patient all the information they require to allow them to give their informed consent to this request.

8.5.4 The practice manager must ensure the request for the transfer of notes is forwarded within 10 working days of the patient giving their informed consent to the request.

8.5.5 On receipt of the notes reception will ensure that the hard copy notes are placed in the tray of the GP the patient is allocated to. This GP is responsible to check the notes to ensure classifications, etc. are completed. Electronic notes are forwarded to the particular GP.

9. Compliance Notices and Criminal Offences

9.1 The OPC can issue compliance notices. The notice will describe the steps required to remedy non-compliance. Failure to adhere to a compliance notice can result in a fine of up to $10 000.

9.2 The Act (2020) introduces two criminal offences

9.2.1 It is an offence to mislead an agency to access, destroy or alter someone else's personal information (e.g. impersonating someone in order to access information you are not entitled to).

9.2.2 It is an offence to destroy personal information, knowing that a request has been made for it.

10. Security of Information

10.1 Staff will ensure that anything displaying or containing health information will be kept away from or out of view of unauthorised people i.e. patient notes and results.

10.2 Patient history and results will be conveyed out of public areas. Patients are taken into a separate room with a nurse where appropriate.

10.3 Filing cabinets, storage areas and unattended rooms will be locked when not in use and access restricted to authorised personnel.

10.4 Reasonable security safeguards should be made to protect the loss, unauthorised access, use, modification or disclosure of health information; this being either electronically (laptops, TXT2Remind, email, storage, shared electronic health record, patient portal), operationally (confidentiality agreements for staff and contractors) and physically (entry, whiteboard, computers, storage).

10.5 When a staff member is no longer employed by the practice, keys must be returned and alarm codes will be changed.

10.6 Any information identifying patients or staff, no longer required by the practice will be destroyed in a manner which prevents identification of the patient or staff member.

10.7 All documents with patient identifiable information go into a shredding container that is provided in every room. This is emptied into the shredding wheelie bin stored in the reception area. This is collected on site by Proshred company every two weeks for shredding.

10.8 If a breach occurred Victoria Clinic has to assess whether the breach reached the “serious harm” threshold.

11 IT Systems

11.1 Computer passwords will be used.
All passwords, account names, tokens or log in identifications required to access software should be kept secure and confidential.

11.2 Passwords should not contain personal details such as date of birth, children’s names etc. Passwords should be forced to expire and a history maintained to prevent re-use.

11.3 The practice manager will set levels of access so that staff can only access information applicable to their patients or area of activity. These should be reviewed periodically.

11.4 Automatic log off after periods of inactivity and use of screen savers are recommended. Users must log off your computer after use.

11.5 The practice manager will ensure back-up systems for information recovery are in place. The backup media should be sufficiently protected to prevent unauthorised restoration outside of the practice.

11.6 Facsimile header sheets will contain a facsimile caution.

11.7 When upgrading computer hardware all data will be wiped clean using suitable proprietary software.

11.8 Any permanent connections should be made through a secure firewall.

11.9 Any remote connections to the practice should be done via a secure medium such as VPN or other encrypted technology.

11.10 Patient personal details should not be emailed outside of the practice unless sufficiently protected and encrypted.

11.11 The practice manager will ensure the practice has anti-virus software running to minimise the chance of automatic emailing outside of the practice without the author's consent. Victoria Clinic has a hosted solution through Mprove. Mprove is responsible for maintaining anti-virus capabilities.

11.12 Practices should have a procedure in place in the event of a virus or unauthorised intrusion of their data systems. Victoria Clinic's IT service is provided by Mprove and Mprove is responsible to ensure sufficient and efficient anti-virus software to protect the integrity of Victoria Clinic database.

12 Other Privacy Act 2020 changes

12.1 An overseas entity carrying on business in NZ must comply with the Act. They do not need a physical presence in NZ.

12.2 The Act regulates how personal information is sent overseas.

12.3 Agencies should only collect personal information when necessary.

12.4 Refusing access requests – There are some new expectations for refusing access to personal information. These reasons include among others a serious threat to life or safety, or threat of serious harassment.

13 Staff Training

13.1 All staff will undergo training on the need for security of patient records, including when information may be accessed, used and disclosed. Initial training will occur as part of the staff orientation programme. Ongoing training will be provided to meet practice and individual staff member's needs.

13.2 Staff should be aware of current security policies regarding non-disclosure of passwords or user names on the telephone to unidentified persons.

13.3 Access to practice computers should only be given to authorised persons.

13.4 Staff are discouraged from making data portable through portable media e.g. data sticks. The Privacy officer must be consulted before any information identifying staff or patients is copied to portable media.

13.5 Staff are discouraged from installing non-essential software either from their own personal sources or internet, onto their practice computers.

14 Errors / Complaints

Victoria Clinic
Urgent Care Standard 2015- Indicator 1.2.1
Privacy Policy
RNZCUC & RNZCGP

All incidents and errors relating to the implementation of the complaints policy will be recorded and managed as per the practice's incident management policy.

The incident management policy will be used to evaluate the effectiveness of this policy as appropriate.