HEALTH INFORMATION PRIVACY

Purpose

This document outlines the policy related to the Privacy, in line with the Privacy Act, which promotes and protects the privacy of information collected from and about an individual and the Health Information Privacy Code, which was established specifically for the management of information relating to health and disability support services such as general practice.

Scope

All staff

Policy of the Practice

The practice team members will understand comply with and implement the requirement of the Health Information Privacy Code 1994 and as outlined in this document which state the processes to be followed by the staff in handling health information.

- The practice will have a privacy officer who has received training and is aware of his/her responsibilities.
- The practice will collect, use, store and share health information in a manner that complies with the Health Information Privacy Code 1994 and personal information with the Privacy Act 1993 (replaced by Privacy Act 2020)

All practice staff must:

- Comply with Health Information Privacy Code requirements when using health information and the Privacy Act when using personal information.
- Comply with the Health Information Privacy Code when storing and destroying health information and the Privacy Act with personal information.
- Comply with Health Information Privacy Code requirements when disclosing health information.
- Comply with the Health Information Privacy Code when correcting health information
- Follow the process outlined when dealing with requests for information.
- Ensure confidentiality of information.
- Follow the process outlined to deal with transferring patient's information.
- Have completed training to ensure they understand and comply with Privacy legislation as part of their orientation to the practice.

- Display a privacy poster/notice in the waiting room and/or via TV PowerPoint.
- Have brochures/leaflets relating to privacy available for patients on request in the Important Notices blue folder by bookshelf in waiting room.
- Advise new enrolled patients of the privacy brochures/leaflets made available for them to take, if need to and offer them the MOH Privacy information sheet.

Key reforms in the Privacy Act 2020 (Post December 2020)

- **Mandatory notification of harmful privacy breaches**. If organisations or businesses have a privacy breach that poses a risk of serious harm, they are required to notify the Privacy Commissioner and affected parties. This change brings New Zealand in line with international best practice.
- **Introduction of compliance orders**. The Commissioner may issue compliance notices to require compliance with the Privacy Act. Failure to follow a compliance notice could result a fine of up to $10,000.
- **Binding access determinations.** If an organisation or business refuses to make personal information available upon request, the Commissioner will have the power to demand release.
- **Controls on the disclosure of information overseas**. Before disclosing New Zealanders' personal information overseas, New Zealand organisations or businesses will need to ensure those overseas, entities have similar levels of privacy protection to those in New Zealand.
- **New criminal offences.** It will be an offence to mislead an organisation or business in a way that affects someone's personal information or to destroy personal information if a request has been made for it. The maximum fine for these offences is $10,000.
- **Explicit application to businesses whether or not they have a legal or physical presence in New Zealand.** If an international digital platform is carrying on business in New Zealand, with the New Zealanders' personal information, there will be no question that they will be obliged to comply with New Zealand law regardless of where they or their servers are based.

Privacy Officer Responsibilities

Each team member is responsible for ensuring that this is up to date and trained in privacy issues.
The responsibilities of the Privacy Officer include:

1. Ensuring that the practice has the required privacy policies and procedures up to date and stored in a readily accessible format.
2. Ensuring that all team members have read and understood the policies and procedures and have updated their personal training record to that effect.
3. Ensuring that the practice complies with the Privacy Act in relation to employees, and the Health Information Privacy Code in relation to patient information.
4. Dealing with requests made to the practice about personal or employment information.
5. Briefing the practice team on changes to practice processes
6. Alerting the practice team to privacy complaints received and what will be done to prevent the same thing happening again.
7. Up skilling the practice team on workshop information / case studies (i.e. providing training in practice team meetings).
8. Overseeing the Orientation (privacy) process.
9. Advising management about recommended training opportunities to up skill the practice team.
10. Ensuring training records are up to date.
11. Ensuring that the privacy complaints received are dealt with in the correct manner and working with the Privacy Commissioner or investigating officer should the need arise.
12. Ensuring that there are clear guidelines on who can access patient information and that handling health information is done according to practice policies and procedures.
13. Notification of any harmful preaches via Privacy website
https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/

The 12 Health Information privacy rules

1. Purpose of collection of health information
2. Source of health information
3. Collection of health information from individual
4. Manner of collection of health information
5. Storage and security of health information
6. Access to personal health information
7. Correction of health information
8. Accuracy etc of health information to be checked before use
9. Retention of health information
10. Limits on use of health information
11. Limits on disclosure of health information
12. Unique identifiers

Confidentiality

This will be ensured by the use of the Privacy legislation and with duty of medical practitioners to maintain confidentiality, and by having signed confidentiality agreements with all staff and contractors

Management of Confidential Waste

Confidential waste is shredded-collected. If large amount of confidentiality waste is anticipated a document destruction bin is ordered.

Displaying of Poster

Health Information Privacy notice is displayed on (TV screen in waiting room OR in waiting room etc)

Brochures

Good Privacy is good Business and Health Information Check–up.
Available at no cost through the Privacy Commissioners Office 04 4747590 / 0800803909
A copy of the health information privacy Act is to be held by the privacy officer for the practice

Training

The privacy officer for the practice must undertake the online privacy training Privacy 101 and Health 101 via the Privacy commissioner's website. Other staff may choose to complete the training available via the privacy commissioner's website, or the PHO website or in-hours session held by the practice privacy offer. Evidence of training must be held by the practice. As new staff are employed, they will need to demonstrate that they have undertaken recent training relevant to general practice.
There is no timeframe for the validity of training, however good practice is to provide staff with refresher courses every 3-5 years.

Security Camera

The practice has a security camera in place, signage is on display on TV screen informing consumers of the cameras,
The cameras will only be viewed if there is an issue and only by the practice principals.

Secure PMS

Each staff should have their own unique login name protected by a password that is at least 8 characters long consisting of mixed alpha and numerical characters. Password will be automatically reminded to change every 90 days by PMS system.

Data Securities - Portal Access

The practice portal uses SSL security technology and is hosted in a secured offsite sever by the company.
Patient registration for the portal can be done while in the practice or if they prefer, instructions will be sent via nominated email address/mobile number once **consented and nominated email/mobile number is added on the enrolment form.**
Once a patient has read and agreed, an **activation code** will be sent to the nominated email/mobile number.
The Patient will need to click on the link sent via email to activate their registration *or* enter the code sent via mobile number and follow the instructions online.
This completes the consent to use the portal for booking appointments; checking results, request repeat prescription and; send secured email messages to the clinical team.

Staff access to the portal is through secured PMS login.
Staff login passwords are set up to be automatically reminded to change every 90 days by system.
If a staff member leave the practice the Practice manger is responsible for removing the ex-staff member's access details.

- For Portal users – see (Health365/MedTech/ConnectMed) Portal policy

Other Important Resources

1. Office of the Privacy Commissioner – telephone 0800 803 909 or www.privacy.org.nz
2. Privacy Act 1993
3. Health Information Privacy Code (HIPC)1994
4. Employment Relations Act 2000
5. On the Record, a Practical Guide to Health Information Privacy, 2nd edition
6. Medical Council of New Zealand – The maintenance and retention of patient records
7. Medical Protection Society 0800 225567
8. Portal security site www.lapageconsulting.com