****

# HEALTH INFORMATION SECUIRTY POLICY

**Context**

Churton park Medical Care (CPMC) ensures that patient's health information is keep confidential, secure and understands that health information is collected by health providers in a situation of confidence and trust.

The collection, use, storage, disposal, processes, and technology in managing health information complies with to the [Health Information Privacy Code 2020](https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Health-Information-Privacy-Code-2020-website-version.pdf), [Information paper on Changes to Notified Code Jul 2020](https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Information-Paper-on-changes-to-the-notified-Health-Information-Privacy-Code2.pdf), and the [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html).

**Policy Objectives**

* To define Churton Medical Park Care approach to managing and securing confidential health information and other personal information.
* To define accountabilities and responsibilities within CMPC for managing privacy and confidentiality.
* To ensure all staff know and understand the importance of the 13 rules of the Health Information Privacy Code 2020. The rules in the code are summarised as:

1. Only collect health information if needed.
2. Retrieve information straight from the source.
3. Advise what the information would be used for.
4. Be considerate when retrieving information.
5. Take care of the collected information.
6. People can see their health information if they want to.
7. They can correct the information it if it is wrong.
8. Make sure health information is correct before it is to be used.
9. Securely discard of the information if no longer needed.
10. Use the information for the purpose it was intended for.
11. Only disclose if there is valid reason
12. Disclosure of health information outside New Zealand
13. Only assign unique identifiers where permitted

**Overarching Principals**

***Storage and information security***

* The practice ensure systems and processes for storage, transmission and disposal of health information are designed to reduce risk of unauthorised access, modification, disclosure, or loss.
* The practice ensures the disposal of physically stored (paper) health information is correctly discarded either by Shredding and/or Locked destruction bin.
* The practice ensures the disposal of electronically stored health information is correctly discarded
* The practice ensure access to health information is restricted to only those people who need access to do their job.
* ensures personal and other confidential information is held through management of an inventory of repositories.
* The practice does not keep information longer than necessary and will dispose of it securely as soon as it is no longer needed
* Only retain information beyond the time required for the original purpose if there is long term research value in doing so.
* Implement regular audits to identify unauthorised access (e.g., staff accessing information relating to other staff or high-profile people).
* CMPC ensures any breaches, incidents and near misses are reported as soon as possible after detection. In the event of a breach, the practice will take immediate action to contain the breach.

***Practice management system***

Most sensitive information is stored in the Practice Management System MedTech. MedTech meets the requirements for digital health information security and provides:

* Information capability to support healthy population
* Information systems to support proactive primary care
* Clinical decision -making support
* Coordinate care system to support timely quality treatment
* Other integrated systems capability such as;
* Standardised e-Referrals
* E-prescriptions, patient portals, shared care records
* Processes and capability to access data across multiple providers and disciplines
* Transactions and Integrated funding arrangements
* Transfer of health records

To access the practice PMS system requires a personal login ID and password. To protect against any unattended access, the system will automatically require a password or an alternative password-protected screensaver to access the computer, or terminal after a period of inactivity.

All computer monitors should be positioned so the screens cannot be seen by patients or unauthorised personnel.

Staff using to the PMS are assigned with appropriate level of system access needed to fulfil their roles and duties.

***Security of digital platforms***

The practice offers telephone consults. Prior to a phone call from a GP (General Practices) or nurse is recommended to establish whether the consult can be done by video or telephone and ensures patient understands:

* Informed consent is obtained (e.g. verbally) and attached to the patient files in the PMS
* GPs (General Practitioners) and Nurses document in the patient notes the type of consult undertaken
* Explain how test results or diagnostic information will be communicated

To maintain patient confidentially, privacy and security of patient information during video or telephone consults is included in the current Privacy Policy.

***Back up and retrieval system***

Back up files and patient information are kept and stored securely, and its purpose is to recover all patient information stored in the computer system in an event of a catastrophic loss of system.

***Handling of a new patient medical records***

Efficient and secure handling of newly enrolled patient medical information is essential for continuity of care from one provider to another, and ensures the patient’s new provider is aware of and follows up anything coming up due or overdue

The practice ensures newly enrolled patients records are reviewed by a clinician and follows a patient management process. Secure handling of new patient records is included in the Records Transfer Policy.

***Tracking of health records***

The practice uses (GP2GP) and electronic system which can transfer records securely and accurately electronically.

The practice ensures that any hard copy health information transferred between providers reaches the intended recipient and is tracked. Example of a tracking receipt of health records may include:

* A fax-back form
* A secure email with a form of acknowledgement
* Use of registered mail or courier packs with a signature (use of standards post services is not considered secure).

To process and transfer patient records, securely and efficiently is included in the Health records Transfer policy and procedure

## **Responsibilities**

***All staff***

* Take responsibility for health and other confidential information they have access to
* Understand the principles, policies and procedures relating to management of personal, health and other confidential information.
* Are clear about their obligations, the expectations on them, and the processes and procedures that are relevant to their work.
* Attend relevant training within their scope of work.
* Report breaches, incidents and near misses.

***Personal information owners***

* Ensure adequate training and resources are available for staff understand the policy and the supporting guidelines, processes and procedures and putting them into practice.
* The practice determines training staff relevant to their roles.
* Maintain and manage this policy, and any other related documents
* Identify the need for guidelines, processes, and procedures to be revised or new ones developed.

**Resources:**

* Health information Security Framework: [https://www.health.govt.nz/about-](https://www.health.govt.nz/about-ministry/leadership-ministry/expert-groups/health-information-standards-organisation) [ministry/leadership-ministry/expert-](https://www.health.govt.nz/about-ministry/leadership-ministry/expert-groups/health-information-standards-organisation) [groups/health-information-standards-](https://www.health.govt.nz/about-ministry/leadership-ministry/expert-groups/health-information-standards-organisation) [organisation](https://www.health.govt.nz/about-ministry/leadership-ministry/expert-groups/health-information-standards-organisation)
* Code of Health and Disability Services Consumers Rights: [https://www.hdc.org.nz/your-](https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights/) [rights/about-the-code/code-of-health-](https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights/) [and-disability-services-consumers-](https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights/) [rights/](https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights/)
* Health Information Privacy Code 2020 <https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/>
* Information paper on changed to the HIPC (Health Information Privacy Code) 2020 <https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Information-Paper-on-changes-to-the-notified-Health-Information-Privacy-Code2.pdf>
* privacy Act 2020 <https://www.privacy.org.nz/privacy-act-2020/privacy-act-2020/>
* Top 11 cyber security tips for your business cyber <https://www.cert.govt.nz/business/guides/business-basics/top-11-cyber-security-tips-for-your-business/>
* Human Rights Act 1993 <https://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html>

|  |  |
| --- | --- |
| Policy name | HEALTH INFORMATION SECUIRTY POLICY |
| Policy Owner | Beverley Downes – Practice Manager |
| Foundation | Indicator 2.1 |
| Date reviewed | April 2024 |
| Date of next review | April 2027 |