
Secure Management of Patient Health Information

1. Introduction

This policy outlines the procedures and protocols to be followed by all staff at Eaglehawk GP Clinic in relation to the secure management, transmission, and sharing of patient health records. This policy ensures compliance with privacy regulations, maintains patient confidentiality, and safeguards patient health data from unauthorised access.

2. Objectives

The main objectives of this communication policy are to:

Protect patient health records from unauthorised access, disclosure, alteration, or loss.

Ensure all communications involving patient health information are secure.

Maintain compliance with the Health Records Act, Privacy Act, and any other applicable legislation.

3. Confidentiality and Privacy

All patient health information is considered confidential. The confidentiality of patient records must be respected and always maintained by all personnel at Eaglehawk GP Clinic. Health information should only be shared with authorized individuals for legitimate medical, administrative, or legal purposes.

Access Control: Access to patient health records is to be restricted to staff who require it for their role. Records are secured and logged.

Training: All staff undergo regular training on patient confidentiality, data security, and the legal implications of breaching confidentiality.

4. Methods of Secure Communication

All communication involving patient health records must be conducted using secure methods to prevent unauthorised access or data breaches.

Secure Management of Patient Health Information

5. Electronic Communication

Email: Any email containing patient health information is encrypted. If encryption is not possible, health information will not be sent via email.

File Sharing: Patient health records are stored in secure, password-protected systems.

Any file sharing must be done via secure channels

Paper Communication

Physical Records: Eaglehawk GP Clinic does not use paper-based records and if we receive paper records, they are imported and then the original copy is destroyed.

Patient information is never to be left unattended or exposed.

Fax: When sending faxes containing sensitive patient information, we ensure fax numbers is correct and that a cover sheet indicating confidentiality is used.

Telephone Communication

- **Verifying Identity:** Before discussing any patient health information over the phone, the identity of the caller must be verified using secure verification questions.
- **Confidentiality:** Sensitive patient information should not be shared on speakerphone or in public areas where others may overhear.

6. Data Retention and Disposal

All patient health records, whether electronic or paper-based, must be retained in accordance with relevant legal and regulatory requirements. Once records are no longer required or have exceeded their retention period, they are securely destroyed.

- **Electronic Records:** When no longer required, electronic records must be deleted securely using methods that prevent recovery of data.
- **Paper Records:** Paper records should be shredded or destroyed using secure methods to ensure patient information is irretrievably lost.

Secure Management of Patient Health Information

7. Third-Party Providers

All third-party service providers, including contractors, cloud storage providers, and business associates, must adhere to the same privacy and security protocols as Eaglehawk GP Clinic. Data-sharing agreements are in place to define the security measures and responsibilities of these providers.

8. Monitoring and Auditing

To ensure compliance with this policy, regular monitoring and auditing of communications and systems will be conducted. This includes:

- Monitoring access logs to detect unauthorised access.
- Reviewing electronic communications to ensure secure methods are being used.
- Regularly testing backup systems to ensure data integrity.

9. Incident Reporting and Breaches

Any breaches of this communication policy, including unauthorised access to patient records or data loss, must be immediately reported to the Practice Manager. An investigation will be conducted to assess the scope of the breach, and corrective actions will be taken.

10. Policy Review

This communication policy will be reviewed annually to ensure its effectiveness and compliance with changing regulations and best practices in data security.

11. Conclusion

The security and confidentiality of patient health records is of paramount importance. All staff must adhere to the practices and guidelines outlined in this policy to ensure Eaglehawk GP Clinic maintains the highest standards of data protection and patient care.