Sapphire Clinic Policy – Privacy and Confidentiality

Effective Date: 07/07/2024
Review Date: June 2025

Introduction

Sapphire Clinic is dedicated to safeguarding the privacy and confidentiality of patient health information in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 and relevant state legislation. This Privacy Policy outlines our approach to managing personal health information, ensuring it is handled with care and compliance.

In developing and reviewing our privacy policies, we carefully assess compliance with all current privacy requirements and legislative updates. We prioritise educating team members about their responsibilities in handling patient health information securely, while also addressing the risks inherent in maintaining health records. Additionally, we ensure robust security measures are in place for our computer systems and electronic communications, and we maintain clear policies governing the use of email, social media, and the secure transfer of patient health information.

Definition of a Patient Health Record

A patient health record is a comprehensive record that includes personal health information, medical history, treatment details, and any other information relevant to the patient's healthcare. This record is used to support ongoing treatment and care.

Collection of Personal Information

The practice collects and holds the following types of personal information:

- Personal details: name, address, date of birth, gender, and contact information.
- Medical history: past and current medical conditions, medications, treatment plans, and immunisation records.
- Medicare and health insurance details.
- Consultation notes, test results, referrals, and any correspondence related to patient care.

We collect personal information:

- Directly from patients or their authorised representatives.
- From other healthcare providers, with patient consent.

Use of Personal Information

Personal information is used for the primary purpose of providing healthcare services, which includes:

- Diagnosis and treatment

- Referral to specialists and allied healthcare providers

- Management of medical records

- Billing and payment processes

We may also use personal information for related purposes where the individual would reasonably expect us to do so, or where permitted or required by law.

Disclosure of Personal Information

We may disclose personal information:

When: Personal information may be disclosed when necessary for the provision of healthcare services, including but not limited to:

- Sharing medical information with specialists or allied health professionals involved in patient care.

- Providing information to pathology or imaging services for diagnostic purposes.

- Sharing information with billing and insurance providers to process payment claims.

Why: Personal information is disclosed for the primary purpose of providing healthcare services and related administrative functions. This includes:

- Ensuring continuity and quality of patient care.

- Facilitating communication among healthcare providers involved in patient treatment.

- Complying with legal and regulatory requirements, such as mandatory reporting obligations.

With Whom: Personal information may be shared with:

- Healthcare providers directly involved in patient care.

- Third-party service providers who assist in providing healthcare services (e.g., IT support, medical transcription services).

- Government agencies or authorities as required by law (e.g., Medicare, public health authorities).

- Insurance providers for billing and reimbursement purposes, with patient consent or as required by health insurance contracts.

Storage and Protection of Personal Information

Sapphire Clinic store personal information securely, using encrypted electronic systems and secure physical storage for paper records.

Sapphire Clinic take all reasonable steps to ensure that personal health information is protected from misuse, interference, loss, unauthorised access, modification, or disclosure. This includes:

- Securing electronic health records with password protection and encryption.
- Restricting access to personal information to authorised personnel only.
- Implementing physical security measures for paper records.
- Regularly reviewing and updating our information security practices.

Personal health information is retained in accordance with legal requirements, after which it is securely destroyed.

Anonymity and Pseudonymity

Patients have the option to communicate with the practice anonymously or under a pseudonym, where it is lawful and practicable. However, in some cases, this may limit the services we can provide.

Accessing and Correcting Personal Information

Patients can request access to their personal health information by submitting a written request. We will respond within a reasonable time frame and may charge a fee for providing access. If any information is incorrect, patients can request corrections.

Complaints About Privacy Breaches

If a patient believes there has been a breach of the APPs or a registered APP code, they can lodge a complaint with our Privacy Officer, The Practice Manager, at manager@sapphireclinic.com.au. We will investigate and respond to complaints promptly, in accordance with our complaints handling procedure.

If you are not satisfied with our response, you may escalate your complaint to the Office of the Australian Information Commissioner (OAIC). The OAIC can be contacted at www.oaic.gov.au or on 1300 363 992.

Informed Consent for Disclosure of Health Information

We obtain informed consent from patients before disclosing health information to third parties, except where required by law. This includes disclosures to other healthcare providers, insurers, or legal representatives.

Disclosure of Health Information

Health information may be disclosed to:

- Other healthcare providers for treatment purposes.
- Insurance companies, with patient consent.
- Government agencies, where legally required.

If health information will be disclosed overseas, patients will be informed of the countries involved and the protections in place to secure their information.

Document Automation Technologies

Our practice uses document automation technologies to streamline administrative processes, including the creation of referral letters. These technologies are configured to ensure only relevant and necessary medical information is included, maintaining the confidentiality and accuracy of patient data.

Real-Time Recording and Telehealth Consultations

For consultations conducted via Telehealth or those that may involve real-time audio/visual recording, duplication, or storage, we obtain informed consent from patients prior to the session. This ensures that patients are fully aware of and agree to the recording and storage of their consultation.

Availability of Privacy Policy

This Privacy Policy is available to patients upon request and can be accessed via our website Sapphire Clinic or at our practice.

Staff Training and Compliance

All staff members receive privacy training at the time of induction and as part of regular ongoing training. This ensures that all team members understand their responsibilities in managing patient health information securely and in compliance with the APPs.

Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in legal requirements or our practices. The updated policy will be posted on our website and made available at our practice.

Related Documents

Sapphire Clinic Statement - Privacy and information management

Sapphire Clinic Complaints and Compliments Policy

Sapphire Clinic Standards-Compliant Secure Messaging Capability