St George Private Radiology

Trading as

Dr Glenn and Partners Medical Imaging

and

Pacific Imaging Maroubra

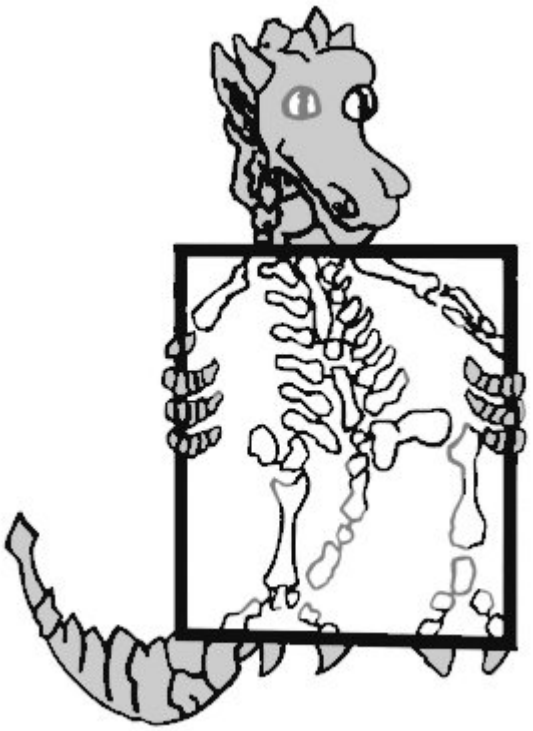

Table of Contents

1. Introduction

St George Private Radiology upholds the thirteen Australian Privacy Principles (**APP's**) outlined in the Privacy Act (**the Act**). APP's apply to all private and public entities from March 2014.

This APP Privacy Policy explains;

a) The kinds of personal information that St George Private Radiology Pty Ltd (hereafter referred to as "the Company") holds,

b) How the Company collects and holds personal information,

c) Matters related to anonymity and pseudonymity,

d) The purpose for which the Company holds, collects, uses and discloses personal information,

e) How an individual may access personal information about the individual that is held by the entity and see the correction of such information,

f) How an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the Company, and how the Company will deal with such a complaint,

g) Whether the Company is likely to disclose information to overseas recipients,

h) If the entity is likely to disclose personal information to overseas recipients - the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

2. Personal Information held by the Company

1. Patients and/or Prospective Patients

Information we commonly collect about patients includes but is not limited to:

- Name, gender, address and other contact details
- Medical history
- Medicare, pension, health care card and other government identifiers
- Family, social and employment history and circumstances
- Health services requested or provided and the outcome or results
- Billing information/history
- Expressed wishes about the future provision of health services
- Details of feedback, complaints, suggestions

2. Referring Clinicians, Practice Managers and Staff

Information we commonly collect about referring clinicians, practice managers and staff, includes but is not limited to:

- Name, address, telephone numbers, fax /email address and other contact details
- Details of IT systems and web addresses
- Medicare provider numbers and billing information
- Area of specialty
- Employment history
- Service delivery preferences, referral patterns and fees paid by referred patients
- Information gathered by client services/marketing staff during practice visits/interactions
- Expressed wishes about the future provision of health services
- Service improvement comments/preferences
- Details of feedback, complaints, suggestions

3. Staff

Information we commonly collect about Staff includes but is not limited to:

- Name, address, telephone numbers, email address and other contact details
- Employment records
- Tax File Records
- Performance records

4. Employment Applicants

Information we commonly collect about employment applicants includes but is not limited to:

- Name, address, email address and other contact details
- Letters of application/expressions of interest and associated correspondence
- Curriculum Vitae/Resume
- Referee comments

5. Anonymity and Pseudonymity

It is impractical for persons to deal with the Company anonymously or by using a pseudonym. This is because:

- diagnosis and/or advice may be seriously impaired
- it might cause an unacceptable risk to patient safety and would conflict with Commission on Safety and Quality in Healthcare's Patient Identification Safety Standards
- there is an unacceptable risk of communication breakdown between the Company and a patient's treating physician
- it may result in a breakdown in good Public Health practice
- examination may not be claimed under Medicare or Private Health Funds

3. How the Company Collects Personal Information

The Company collects personal information by the following means:

- Face to face
- Telephone
- Email and other electronic means
- Fax

4. Solicited vs Unsolicited Information

Most of the personal information collected by the Company is solicited. On occasions the Company may receive unsolicited information. If unsolicited information is received the principals outlined in this policy will still apply.

5. How the Company Holds Personal Information

The Company commonly holds personal information in the following mediums:

- Electronically
- Hard copy
- Digital audio recordings
- Digital and hard copy images
- Paper based and other hard copy documents located securely within the practice.
- Contained in electronic records in a secure environment; and
- Archived in dedicated secure storage facilities.

6. Security of Personal Information

The Company has procedures in place to store personal information securely to protect from unauthorized access, disclosure, misuse, loss and modification.

Processes include but are not limited to:

a) Hard copy documents are located securely within the practice or secure storage centers.

b) In electronic databases in a secure environment; and in a secure archive storage facility

c) Records are only accessible by persons who require access to that information for the purpose of carrying out their employment

d) Hard copy documents securely destroyed using a dedicated third party document destruction service

e) Incident reporting of data security breaches

f) Strong internal governance practices

g) Staff training

h) Regular review of policy and procedures.

7. How the Company Uses Personal Information

The Company may collect personal information;

a) For the primary purpose for which it was collected; or
b) For directly related secondary purposes which we believe are within your reasonable expectations; or
c) In a manner for which you have given consent

As required for the provision of our service the Company may collect Sensitive Information as defined in the Privacy Act.

1. Patients

1. Primary Purposes

- To provide reliable healthcare services
- To link medical records of patients to their healthcare provider
- Ensure appropriate testing
- Diagnose and interpret results
- Allow billing and payments
- If lawfully instructed to reveal information;

2. Secondary Purposes

- For our internal administrative requirements, including for management purposes, funding, service monitoring, planning, evaluation and accreditation activities
- To provide data in both an identified and de-identified form to State and Federal Government agencies in compliance with numerous legislative requirements (e.g. Breast Screen, Cancer Council, National Health and Medical Research Council)
- For complaint handling and defense of anticipated or existing legal actions
- To our insurers, brokers, lawyers and other experts for the purposes of addressing liability indemnity arrangements or to obtain advices as to our legal or other obligations
- For planning and evaluation of accreditation activities and with our professional bodies
- for teaching purposes, case studies and multidisciplinary clinical team meetings in de- identified form
- For provision of further information about medical advances in pathology/radiology and treatment option
- If your health information is used or disclosed for one or more of these purposes, we will not normally seek your specific consent.

3. Uses Requiring Patient Consent

The Company will obtain your consent if your health information is proposed to be used or disclosed without de-identification for:

- Marketing, and to communicate special events
- Research

If research is being contemplated, reasonable steps will be taken to ensure you understand what the proposed research involves, the ways in which your health information will be used, and the risks and benefits of agreeing to participate.

2. Referring Clinicians, Practice Managers and Staff

1. Primary Purposes

- To provide reliable healthcare services for patients
- To link medical records to patients and their healthcare provider
- Ensure appropriate testing
- To diagnose and interpret results
- To tailor services to a referrers needs
- To provide educational material to referrers and their staff

2. Secondary Purposes

- Direct marketing via email or mail

8. Disclosure of Personal Information

The Company may disclose your personal information

- For the purposes of getting a second medical opinion
- To a third party health provider or service who is providing direct clinical care to a patient
- To a third party health provider within a hospital campus where an individual is being treated
- Where it may be more appropriate for a test to be performed by a specialist service
- Where there are statutory requirements to report results to registries
- To third parties organisation for billing/accounting purposes

9. An individual's right to control the use and disclosure of personal information.

The Company believes that the use and disclosure of personal information in the ways described in this policy will reflect the reasonable expectations of an individual dealing with us.

An individual may understand the advantages and approve of health information being shared between several health service providers, such as the Company and individual's referring medical practitioner, as part of their overall health treatment and management.

However, sometimes the parties' expectations do not align. For example, an individual may not want a report to be directly sent to the referring medical practitioner following the service.

An individual may also not want the Company to provide certain health information or does not want their health information to be used or disclosed in a particular way.

The Company respects such wishes and will, in accordance with the Act and the APPs, take all reasonable steps to comply with such wishes.

The Company strongly encourages patients to obtain their health information, particularly copies of results from their referring medical practitioner. This is likely to best facilitate effective and efficient delivery of treatment and ensures that the referring medical practitioner has an opportunity to clarify any aspects of the results and to answer any questions or concerns a patient may have. It is the referring medical practitioner who makes the diagnosis. Results provided in isolation may be misleading.

10. Integrity of Personal Information

The Company takes reasonable steps to ensure personal information it holds is:

- Accurate, complete, well organised and legible
- Up to date, in that they reflect the personal information most recently obtained from the individual
- Does not contain prejudicial, derogatory or irrelevant statements

1. For Patients

- All relevant personal information is reconfirmed at each attendance
- The Company fulfils regulatory, accreditation and public health requirements on patient identity

2. For referring practitioners, their staff and other third parties

- Providing mechanisms to update personal information (address, phone, fax, email)
- Receiving feedback via face to face, phone or written contact and updating records accordingly.

11. Access to and Correction of Personal Information

Access

Individuals have the right to access personal information held by the Company. An individual does not have to provide a reason for requesting access.

The preferred method for patients to receive results is in consultation with their treating practitioner where the results can be explained in the context of their health management.

the Company may request that an individual complete a *Request for Information*, in order to ensure that you are given the correct health information. Proof of identity will be required. Processing of applications is normally completed within 30 days.

The Company is not required to provide access to the personal information to the extent that:

1. the Company reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
2. giving access would have an unreasonable impact on the privacy of other individuals; or
3. the request for access is frivolous or vexatious; or
4. the information relates to existing or anticipated legal proceedings between the Company and the individual, and would not be accessible by the process of discovery in those proceedings; or
5. giving access would reveal the intentions of the the Company in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
6. giving access would be unlawful; or
7. denying access is required or authorised by or under an Australian law or a court/tribunal order; or
8. the Company has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
9. giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
10. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
11. giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

12. Correction

If an individual believes information held about them is incorrect, incomplete or inaccurate, then the individual may apply for the information to be corrected by contacting the privacy officer.

The Company may refuse to correct personal information and will provide a written response that sets out:

a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

b) the mechanisms available to complain about the refusal; and

c) any other matter prescribed by the regulations.

13. Request to associate a statement or opinion

a) If the Company refuses to correct the personal information as requested by the individual; and

b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

The Company will take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

14. Trans-border Data Flow

In rare instances the Company may disclose personal information outside Australia. An individual's privacy will continue to be protected as per APP's.

Instances where trans-border disclosure may occur include;

a) where an individual is participating in a clinical trial

b) when requested by a patient's treating doctor overseas

c) when requested by the patient

d) when samples are sent overseas for expert opinion/analysis

Each instance where personal information is sent overseas is unique, in most cases the individual will already be aware of, and consent to, transfer. Where reasonable the individual will be notified of the overseas destination however it is not always practical to specify.

15. Use of Personal Information for Direct Marketing

We may use personal information for marketing directly related to our services. All marketing communication includes instructions on how to opt out of future communications.

An individual may advise us that they do not wish receive direct marketing from us at any time by contacting the privacy officer.

We will not disclose your personal information to a third party for any marketing purposes.

16. Privacy Complaints Process

If an individual feels that the Company has acted improperly or breached the APP's they may make a complaint. Complaints may be lodged in any form (written, verbal, email etc.) to the Company's Privacy Officer. Where reasonable, the Company will respond to privacy complaints within 30 days.

If the complainant is unsatisfied with the response from the Company they may lodge a complaint with the Office of the Australian Information Commissioner.

the Company Privacy Officer Contact Details

St George Private Radiology
C/o Naomi Palsson
PO Box 233
Rockdale NSW 2217

P: 0416 283 037
E: npalsson@medical-imaging.com.au
W: www.medical-imaging.com.au

Office of the Australian Information Commissioner (OAIC)

GPO Box 2999
Canberra ACT
2601

P: 1300 363 992
E: enquiries@oaic.gov.au
W: http://www.oaic.gov.au/

OAIC Online Privacy Complaint Form
https://forms.business.gov.au/aba/oaic/privacy-complaint-/