PRIVACY POLICY
(Patient Information)

Alfred Medical Imaging Holdings Pty Limited (ACN 612 792 560), and its subsidiaries ('AMI', 'the Company', 'we' or 'our') recognises that, as a private sector healthcare provider, it must at a minimum comply with and have obligations under the *Privacy Act 1988* (Cth) (as amended) ('the Act') and as such the Australian Privacy Principles ('APPs') enacted under this legislation.

The Company commits to open and transparent management of personal and sensitive information by way of providing an up to date Privacy Policy, and associated procedures, guidelines and information. The Privacy Policy and affiliated documentation will, at a minimum, outline:

- the kinds of personal and sensitive information collected and held (retained /stored);
- the method by which information will be collected and held;
- the purposes for which personal and sensitive information is collected, held, used and disclosed;
- how individuals can access their personal and sensitive information held by the Company;
- how individuals can keep stored information correct and current;
- the complaints process in place for individuals to register an issue or dissatisfaction with Company adherence to APPs;
- how complaints relating to privacy will be dealt with; and
- the possibility of personal or sensitive information being disclosed to overseas recipients and, where practicable, specific details of potential recipient countries.

Purpose

To comply with the Act and other governing legislation related to information and data.

To ensure all patients' right to privacy is upheld and their personal, sensitive and health related information, is protected.

To foster a privacy and security aware culture among all personnel and contractors providing services on behalf of the Company.

Definitions

Authorised Representative (of patient) *- a person with enduring power of attorney, a legal guardian, parent for children under 18 years of age when those children lack capacity, and other persons authorised by law to represent the patient.*

Company *– Alfred Medical Imaging Holdings Pty Limited, its subsidiaries and trading entities.*

Company Patient Related Privacy Policy – this policy.

Personal Information *– information that identifies a person, or could be used to be used to identify a person, whether on its own or with other information.*

Sensitive/Health Information *- personal information collected for the purpose of healthcare and/or personal information or an opinion about a person's physical health, mental health, disability, health services provided or planned. For the avoidance of doubt, all information collected from patients in Company sites is deemed health information from a legal perspective.*

Scope

PRIVACY POLICY
(Patient Information)

The Company Patient Related Privacy Policy relates to current and former patients of the Company.

The Company Patient Related Privacy Policy relates to all personal, sensitive (non-health related) and health related information.

This Company Patient Related Privacy Policy should be read together with the Company's Privacy Statement, which is available online at https://www.alfredimaging.com.au/privacy, or in hard copy upon request.

The Company Patient Privacy Policy applies to information:

- obtained for use by the Company; and,
- contained within patient records provided for and generated by the performance of services.

Kinds of personal and sensitive information collected

AMI limits the collection of personal, sensitive and health information from patients to that deemed necessary to provide compliant services, optimise diagnosis, assess the appropriateness of referred examinations, and assess the safety of referred examinations or procedures.

To protect the privacy of patients and prospective patients, AMI commits to taking all reasonable steps required for the lawful and reasonable collection, use, storage and disposal of personal and sensitive information, and the protection of personal information AMI holds from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Personal details deemed necessary to collect, store and use, and therefore staff are authorised to collect and use are:

- name;
- address;
- date of birth;
- Medicare, pension and concession, unique identifiers;
- signature; and
- billing related financial or account information.

Health related information (sensitive information), deemed necessary to collect, store and use, for the purposes of optimising the diagnosis, assuring appropriateness of the referred examination and safety of the examination or selected protocol.

Therefore, health related details staff are authorised to collect and use are:

- previous imaging;
- allergies;
- symptoms;
- medical history;
- family medical history;
- medications;
- pregnancy status;
- medical records relating to requested services or services undertaken; and

- radiology reports.

Policy

Privacy related directives should be read and applied in conjunction with Company generated Waste Management and Record Management directives; as well as Company supplied ancillary documentation, including the Company's Privacy Statement (available online at https://www.alfredimaging.com.au/privacy).

- The Company will assist staff in interpreting their rights and responsibilities under the Act by way of training and the provision of practical methods of interpreting the Company Patient Related Privacy Policy and Privacy Statement, including but not limited to, procedures, guidelines and forms.
- The Company commits to making the Company Patient Privacy Policy available to external persons and entities upon request.
- The Company commits to reasonable steps required for:
  - the lawful and reasonable collection, use, storage and disposal of personal and sensitive information.
  - the protection of personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.
- All Company personnel must abide by Company Patient Related Privacy Policy, the Privacy Statement, and associated procedures.
- The Company will provide all patients with written Consent Forms regarding their privacy rights and the Company's intention in relation to the collection, use and disclosure of their personal and sensitive information. Further this consent form will provide general information on security and storage undertakings.
- Company personnel training will include guidance on when and how verbal and implied consent can be attained as well as the steps to take should there be cases where further assistance is needed in relation to access and consent, such case would include access children's medical records/health records.
- Where collection of patient sensitive/health information is needed from other healthcare institutions or practitioners, a Company Third Party Authority to Release consent form should be completed and sent to aforementioned third party. For the avoidance of doubt, a copy of this form should be included in the patient's Company medical record.

<u>Collection</u>

- All patients' information collected or sourced by or on behalf of the Company must be:
  - collected for lawful and Company authorised purposes set out in this Company Patient Related Privacy Policy and Privacy Statement;
  - sufficient for, relevant to, and have a direct bearing on the safe and compliant performance of requested Medical Imaging examinations/procedures;
  - accurate and up to date; and
  - collected following informed consent wherever reasonable and practicable. Exception may only be

made in extreme circumstances where, conforming to consent requirements, would reasonably result in an adverse outcome for the patient.

- Information deemed directly related to the provision of Medical Imaging services includes personal and sensitive data collected for the following purposes:

  - to validate referral information;
  - to ensure correct patient identification;
  - to ensure compliance with MBS in terms of patient status and eligibility;
  - to enable imaging and medical history files to be matched to existing Company unique identifiers and files for review and continuity of care; and
  - to enable imaging and medical history files to be created.

- Where possible, reasonable and practicable personal, sensitive and health related information should be attained directly from the patient. Exceptions accepted by the Company include:

  - in the case of minors where the minor consents to or it is necessary to gain assistance from a parent or legal guardian;
  - in cases where the patient is unconscious or lacks the capacity to provide the needed information where an authorised representative may assist;
  - in cases where family history is relevant and necessary where family members may be required to give accurate and complete medical history;
  - in cases where other healthcare providers have the relevant and necessary information; and
  - in cases where the Company is required or authorised by law, a court or tribunal, to collect information from another person.

- If circumstances arise where the Company or a representative thereof is in possession of unsolicited personal and or sensitive information (information collected outside of the above approved collection methods) and that information is relevant and necessary for the provision of service, staff should determine if they could have collected that information by compliant means. If 'yes' it may be deemed that the collection was reasonable, and the information can be retained and used.

- If circumstances arise where the Company, or a representative thereof, is in possession of unsolicited personal and or sensitive information (information collected outside of the above approved collection methods) and that information is either not relevant or necessary for the provision of service, or staff should determine if they could not have collected that information by compliant means. The information is to be destroyed or disposed of confidentially.

- If circumstances arise where the Company or representatives thereof collect or receive personal or sensitive information lawfully but not directly from the individual, then Company personnel should make best endeavours to notify the person. Notification should include:

  - the collection of their information;
  - the Company identity and contact details;

- the purpose of the information being collected or received (including consequences of not having all necessary information);
- details of any entities or persons that may receive the information, and
- general principles of the Company Patient Related Privacy Policy and Privacy Statement.

Storage, Retainment & Disposal

- Due to the nature of the importance of accuracy and clarity of personal and sensitive information in providing accurate high- quality healthcare, it is impracticable for the Company to afford users of Medical Imaging services anonymity or pseudonymity. Therefore, all records retained on Company systems include personal information or identifiers.

- For the purpose of disposal; all information gathered, and records obtained, produced and/or retained by the Company are considered confidential. Destruction of records is to be in line with such.

- Disposal of hardware that has been used for the purposes of attaining or storing personal or sensitive information must have hard drives destroyed or "cleaned up" as part to the decommissioning process. Company IT personnel are responsible for these processes and adherence to this Company policy requirement.

- The Company retains all patient personal, sensitive and health information for its useful period or as required by legislation only. Due to the nature of services provided by the Company, all medical records are to be kept indefinitely where possible.

Use and Disclosure

- The Company may use and disclose personal and sensitive information from patients in the following ways:
  - conducting or reporting referred Medical Imaging examination(s) and procedure(s);
  - processes directly linked to conducting and reporting specific requested examination(s) and procedure(s);
  - administration tasks and billing and account keeping;
  - disclosure to other health professionals involved in the patient's diagnosis and care;
  - when the Company is bound by law to report or disclose records;
  - disclosure to medical defence insurers;
  - quality assurance activities;
  - training and multi-disciplinary team meetings; and
  - research (please note: a patient's records will be de-identified if used for this purpose and the patient will be made aware of his or her participation by the research instigator or coordinator).

- Under special circumstances, where the Company or its representative/s require the use of any patient information for any other secondary purposes, approval from the Company Chief Executive Officer and informed consent from the subject must be attained. Secondary use includes quality control activities such as image

review. For the avoidance of doubt, authorised access to patient records by Company personnel should be limited to the completion of tasks by the person attending to that task. Company personnel are not permitted to access patient records at any time outside of permitted uses contained herein.

- In the case of release of images and/or reports, a signed Third-Party Authority to Release Consent Form must be obtained for the release of images and/or reports to any party other than the patient or referring doctor.

- All consent and authorisation pertaining to the use or disclosure of patient information and records must be retained in the patient's file (RIS system).

- Disclosure of personal or sensitive information to cross border (international) recipients must:

  - be authorised by a Company Privacy Officer or nominated delegate;be requested by and/or consented* to by the patient, unless disclosure is required or authorised by or under an Australian law, a court or tribunal; and
  - not be disclosed until a signed Company Privacy and Confidentiality Agreement or *equivalent* is received from the recipient, unless disclosure is required or authorised by or under an Australian law, a court or tribunal (equivalent methods include software privacy disclosures and agreement).

  ** Patients requesting cross border disclosure of their private and/or sensitive information are to be informed that although the Company will take reasonable steps to ensure the overseas recipient will not breach Australian Privacy Principles there is a limit to the protection that can be afforded to them once the information is released, as APP 8.1 (concerning disclosure of personal information to overseas recipients) will not apply to the information following the disclosure. The Company will provide relevant information on the Company Personal and Sensitive Information Disclosure Consent Form for use by personnel.*

- The Company may use data and health information for research and training purposes. All patient data used for these purposes must be de-identified prior to use and therefore personal and sensitive information is not to be disclosed. Possible data usage and this Company Patient Privacy Policy is to be provided to all patients at the time of initial registration (via the Company Patient Privacy Consent Form). Patient consent for data use is to be sought at this time. Where patients do not consent to the use of their data, notation should be made in their record to alert relevant personnel.

Accuracy

- The Company commits to taking reasonable endeavours to ensure all data provided by patients is accurate and current. The Company requires signed declarations from all parties disclosing information in the first instance, and accepts updates in good faith. The onus for updating information lies with the subject of such information, that is the patient or parent/legal guardian where relevant.

- Company employees are required to check existing patient files upon subsequent patient visits, and change or update relevant information where the information retained by the Company is inaccurate or incomplete.

- Requests by patients for updated information to be forwarded to third parties are to be accommodated wherever practicable, reasonable and lawful.

- Corrections to personal information are not required to be treated as separate records, uniquely identified or marked as an addendum.

Access

- The Company will grant to the patient access to their information unless deemed inappropriate by law or reasonable assessment. For the avoidance of doubt, inappropriate means that the disclosure or access:

  - would pose a serious threat to the life or health and safety to individuals or the public;
  - would be unlawful; and/or
  - would be provided as part of legal proceedings between the Company and the patient.

- Written requests are required from patients or legal guardians (where applicable) to access retained personal and sensitive information. Where access is granted, information will be provided without unreasonable delay or expense.

- Where access, or the requested manner of access to information is denied, the Company will provide the requestor with written notification of such. Notifications are to include the reasoning for denial and pathways to lodge an objection with the Company.

- Should there be a fee associated with granting access to personal and sensitive information, this will be disclosed at the time of request response.

Security

- The Company takes reasonable steps to retain patient information and records (personal and sensitive data) in a secure manner.
- Company security measures aim to:

  - prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information;
  - detect privacy breaches promptly; and
  - be able to respond to potential privacy breaches in a timely and appropriate manner.

- Due to the nature of Company business, the majority of patient records storage and access pathways are reliant upon IT services. The Company engages both in-house and third-party IT support giving 24 hours 7 day a week access to IT specialists.

- Security measures are in place for both hard and soft copy record retention. Security measures include:

  - employee training in privacy requirements, including but not limited to:
    - measures to protect confidential data; and

- actions that may lead to a potential security breach;

- availability of policies and procedures on data security for all staff;
- regular audit of system and network activity;
- regular testing of defences and security measures; and
- vendor due diligence and contract management as it pertains to data access and security.

IT System Component	Security Measures in Place
Hard Copy Records	• Records retained in restricted access areas
Applications	• User specific password protected access • Access level controlled via defined user groups • Timed lock out after 30 mins inactivity • Access logs for audit – Radiology Information System (RIS) has fully logged access and changes made records
Network	• Network and individual component security measures are in place (refer below)
Firewall	• High availability (HA) cluster configuration with logging of all traffic • Single external user entry point (limited access route) via secure data centre • Restricted access - all traffic limited to ports needed • All access controlled via defined group permissions • Active unified management terminals (UMT) inclusive of geographical blocks in place override user and group access permissions
Router	• Configuration backed up and managed by internet service provider
Switching infrastructure	• Password protected access • Stacked configuration protecting against looping errors and brute-force attacks (using spanning tree)
RIS	*Refer to Applications above*
PACS	• Password protected access • Timed lock out after inactivity • All access controlled via defined group permissions • All external access via HTTPS (secure website with encrypted traffic)
Administration network drives	• Secure network • Off-site access controlled via VPN • Password protected access • All access controlled via defined group permissions
PCs and workstations	• Anti-virus update using SolarWinds monitoring tools and Bitfender scan engine • File server - password protected access with access-controlled group permissions • off-site access controlled via VPN • PC and monitor placement and screensaver activation including log-out timeframes
Imaging Equipment	• Password protected access

IT System Component	Security Measures in Place
	• Equipment shut down / locked outside of business hours and when authorised personnel not in attendance within the restricted area housing equipment • Vendor remote access limited to secure network (VPN) pathways and secure log-in

- Risks to the security of personal and sensitive information is managed through:
  - the use of privacy impact assessments (PIA);
  - security risk assessments;
  - regular reviews of security controls in place;
  - regular IT and security system updates; and
  - system and Privacy Module annual audit.

- Privacy Impact Assessments are required by the Company for all new projects, workflow changes, systems changes and upgrades. Exception is made where a PIA threshold assessment negates the need for a full PIA to be completed.

Data Breaches

- To facilitate best practice in data security and privacy provision to all persons, all systems and equipment used to access, and store sensitive information must have a risk assessment completed at implementation and upgrade.

- A potential data breach is considered to have occurred when sensitive information (personal information and or health related information) is lost or potentially subjected to unauthorised access or disclosure.

- All potential data breaches are to be treated as internally notifiable incidents. As such, all potential data breaches must be reported to the Group IT Manager and Company Privacy Officer (Authorised Person) within 24 hours of the potential breach being identified.

- Investigation into incidents involving potential breaches of the Privacy Act must commence by the Authorised Person or nominated delegate immediately upon receipt of a notification.

- The Company commits to:

  - undertaking reasonable and expeditious assessment of all potential data breaches in order to determine if the potential breach is likely to result in an actual breach and/or in serious harm to any individual affected by that breach;
  - completing assessment of suspected notifiable data breach within 30 days of the breach;
  - take all possible steps to contain the breach; and
  - determine and undertake remedial actions where applicable.

- The Company Authorised Person or nominated delegate will:
    - inform the Office of the Australian Information Commissioner of an eligible data breach (Notifiable Data Breaches as defined in the Privacy Act), and;
    - inform individuals affected by an eligible breach within 24 hours of assessment of the breach or as soon as reasonable practicable if the 24-hour timeframe is not possible.

- Notification to the Office of the Australian Information Commissioner (OAIC) Notifiable Data Breach Form https://forms.uat.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB or alternative OAIC endorsed notification form as varied for time to time.

- Notification to other persons is to be in writing using the Company endorsed Notifiable Data Breach Disclosure Statement by the Company Privacy Officer or nominated delegate.

- At a minimum, notification statements provided to the OAIC will contain:
    - the identity and contact details of the entity;
    - a description of the breach;
    - details of the information subject to the breach; and
    - recommendations for resolution given to individuals affected by the breach.

- All notifiable breaches will be reported to the Company Board of Directors at the time of notification by the Company Privacy Officer or nominated delegate.