SECTION 1 GENERAL INFORMATION

POLICY IM 1.4	PRIVACY POLICY

AIM/OUTCOME: The purpose of this Privacy Policy is to clearly communicate how Presmed Australia Facilities (PMA) handle patients' health information. It will provide a complete understanding of the type of personal information that PMA hold and the way PMA handle that information.

REFERS TO: All Administration Staff
All Clinical Staff
All Accredited Medical Practitioners (AMP's)

POLICY:

We collect information that is necessary to provide patients with health care services. Often this includes collecting information about health history, family history, ethnic background or current lifestyle to assist the health care team in treating the patient's condition.

PMA are committed to ensuring the privacy and confidentiality of patients' personal information. PMA must comply with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and Privacy Amendment Act 2012 (Cth) which govern how private sector health service providers like PMA handle patients' personal information, including health information.

A condensed version of this Privacy Policy is on public display at all Presmed facilities (see Policy 1.4.1 Privacy Policy (Condensed)).

APP1: OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

This Privacy Policy has been developed in accordance with a 'layered policy' format endorsed by the Office of the Federal Privacy Commissioner. This means that it offers the ability to obtain more or less detail about PMA information handling practices.

Basic information about PMA information handling practices is available in the 'condensed' privacy policy, which is on display at all Presmed Facilities [see IM Document 1.4.1]. This is a **summary** of how PMA collect, uses and discloses personal information and how to contact us in order to access or correct any personal information which PMA hold.

This document contains detailed information about PMA information handling practices and is available on their websites.

APP 2: ANONYMITY AND PSEUDONYMITY

In order to provide health care to our patients, PMA needs to collect and use their personal information. If incomplete or inaccurate information is provided to us or health information is withheld from us, PMA may not be able to provide the services required. It is impracticable for PMA to deal with individuals who have not identified themselves or who have used a pseudonum.

APP3: COLLECTION OF PERSONAL INFORMATION

In order to provide patients with required health care services, PMA will need to collect and use patients' personal information.

In this Privacy Policy, we use the terms:

- "Personal information" as it is defined in the Privacy Act 1988 (Cth). This means: *"information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
    - *whether the information or opinion is true or not; and*
    - *whether the information or opinion is recorded in a material form or not";*

  and
- 'health information" as it is defined in the Privacy Act 1988 (Cth). This is a particular subset of "personal information" and means information or an opinion about:
    - the health or a disability (at any time) of an individual; or
    - an individual's expressed wishes about the future provision of health services to him or her; or
    - a health service provided or to be provided to an individual,

  that is also personal information.

Personal information also includes 'sensitive information' which is information such as race, religion, political opinions or sexual preferences, biometric information used for biometric verification or identification, and biometric templates, and health information. Information which is 'sensitive information' attracts a higher privacy standard under the *Privacy Act 1988* (Cth) and is subject to additional mechanisms for protection.

PMA may store the personal information we collect in various forms, including through an electronic medical record system. Personal information may also be stored on some diagnostic equipment where patients have undergone a diagnostic procedure using such equipment in a Presmed facility. PMA will comply with the APPs, and this Privacy Policy, in respect of personal information in whatever form that information is stored by us.

APP 4: DEALING WITH UNSOLICITED PERSONAL INFORMATION

Should PMA receive personal information which was not solicited, it will destroy the information or ensure that the information is de-identified.

APP 5: NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

PMA will usually collect health information directly from the patient. Sometimes, we may need to collect information from a third party (such as a relative or another health service provider). We will only do this if the patient has consented for us to collect information in this way or where it is not reasonable or practical for us to collect this information directly from the patient, such as where their health may be at risk and we need personal information to provide emergency medical treatment. In these circumstances, we will ensure that the patient is notified as soon as possible that said information has been provided by a third party.

APP 6: USE OR DISCLOSURE OF PERSONAL INFORMATION

PMA only uses personal information for the purpose for which the information was provided to us unless one of the following applies:

- The other purpose is directly related to the purpose for which the information was given and the patient would reasonably expect, or we have told the patient, that the information is usually disclosed for another purpose or to other individuals, organisations or agencies
- The patient has consented for us to use their information for another purpose;
- PMA is required or authorised by law to disclose information for another purpose
- the disclosure of information by PMA will prevent or lessen a serious and imminent threat to somebody's life or health; or
- the disclosure of information by PMA is reasonably necessary for the enforcement of the criminal law or a law imposing a penalty or sanction, or for the protection of public revenue.

Use among health professionals to provide treatment

Modern health care practices mean that treatment will be provided by a team of health professionals working together.

Patients may be referred for diagnostic tests such as pathology or radiology and our staff may consult with senior medical experts when determining patients' treatment. Our staff may also refer patients to other health service providers for further treatment during and following their admission

Further, if a patient requires a prosthetic as part of their treatment, we may disclose their personal information to the manufacturer or supplier of that prosthesis.

These health professionals will share health information as part of the process of providing treatment. We will only do this while maintaining confidentiality of all this information and protecting privacy in accordance with the law.

Patients' health information will only be disclosed to those health care workers involved in their treatment.

Risk Mitigation when emailing Patient Personal Information

To mitigate the risk of emailing patient personal information to an incorrect recipient the following actions are to be taken.

- Sender emails only are to be used and accessed from email Contacts List with care taken when selecting the recipient.
- Ensure the email body has no personal data.
- Consider protecting email attachments with a password.
    - Suggested password is facility name abbreviation followed by a space and the year (changed annually). For example CPH 2019 at Chatswood Private Hospital during 2019.
- Read receipts are to be added to the email and acknowledged.

The Patient's Local Doctor

PMA and/or the patient's treating specialist will usually send a discharge summary to the referring medical practitioner or nominated general practitioner following an admission to one of our facilities. This is in accordance with long-standing health industry practice and is intended to inform the doctor of information that may be relevant to any ongoing care or treatment provided by them.

If a patient does not wish to provide a copy of their discharge summary to their nominated general practitioner they must let us know. Alternatively, if their general practitioner has changed or their general practitioner's details have changed following a previous admission, they must let us know.

Other health service providers

If in the future a patient is treated by a medical practitioner or health care facility who needs to have access to the health record of their treatment in one of our facilities we will require an authorisation from the patient to provide a copy of their record to that medical practitioner or health care facility.

The only time we would provide information about patients' health records to another medical practitioner or health facility outside PMA without their consent is in the event of an emergency where the patient's life is at risk and they are not able to provide consent or as approved or authorised by law.

Relatives, guardian, close friends or legal representative

We may provide information about a patient's condition to their parent, child, other relatives, close personal friends, guardians, or a person exercising power of attorney under an enduring power of attorney or who has been appointed enduring guardian, unless the patient tells us that they do not wish us to disclose their health information to any such person.

Other Presmed Australia entities

Presmed Australia may share health information amongst its facilities:

- Chatswood Private Hospital
- Epping Surgery Centre
- Central Coast Day Hospital

- Laser Vision Clinic Central Coast
- Madison Day Surgery
- MetWest Surgical
- Sydney Pain Day Surgery
- Devonport Eye Hospital

For example, this may occur where a patient has been transferred between any of the PMA facilities or to coordinate their care.

Other common uses

In order to provide the best possible environment, we may also use health information where necessary for:

- activities such as quality assurance processes, accreditation, audits, risk and claims management, patient satisfaction surveys and staff education and training;
- invoicing, billing and account management;
- to liaise with health funds, Medicare or the Department of Veteran's Affairs and where required provide information to health funds, Medicare or the Department of Veteran's Affairs to verify treatment provided, as applicable and as necessary;
- the purpose of complying with any applicable laws – for example, in response to a subpoena or compulsory reporting to State or Federal authorities (for example, for specified law enforcement or public health and safety circumstances);
- the purpose of sending standard reminders, for example for appointments and follow-up care, by text message or email to the number or address which has been provided to us.

Contractors

Where we outsource any of our services or hire contractors to perform professional services within our hospitals or health services we require them to also comply with the Privacy Act 1988 (Cth) (or other relevant privacy legislation) and our Privacy Policy.

Other uses with consent

With patients' consent we can also use their information for other purposes such as including them on a marketing mail list, fundraising or research. However, unless we have been provided with express consent for this purpose, we will not use personal information in this way.

CCTV

Presmed Australia may use camera surveillance systems (commonly referred to as CCTV), at its facilities for the purpose of maintaining the safety and security of its staff, patients, visitors and other attendees to those facilities. PMA's CCTV systems may, but will not always, collect and store personal information. PMA will comply with the APPs and this Privacy Policy in respect of any personal information collected via its CCTV systems.

Contracted services

PMA provides some health services to public patients and to groups such as Defence or Customs personnel under contracts with government. Where patients receive services from us under any such arrangements PMA will provide their personal and health information to those government agencies as required under those contracts.

Job applications

PMA collects personal information of job applicants for the primary purpose of assessing and (if successful) engaging applicants.

The purposes for which PMA uses personal information of job applicants include:

- managing the individual's employment or engagement;
- insurance purposes;
- ensuring that it holds relevant contact information; and
- satisfying its legal obligations.

PMA may also store information provided by job applicants who were unsuccessful for the purposes of future recruitment.

Application for accreditation by health professionals

PMA collects personal information from health professionals seeking accreditation and submitting to the credentialing process under the Presmed By-Laws. Personal information provided by health professionals in this context is collected, used, stored and disclosed by PMA for the purposes of fulfilling its obligations in connection with the Presmed By-Laws.

APP 7: DIRECT MARKETING

PMA may involve patients in patient feedback forms, hospital websites and forums, community engagement meetings, health awareness programmes and/or marketing for hospital services.

PMA will only use personal information for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose. Such consent may be express or implied. The option to "opt out" of involvement in direct marketing is clearly and prominently displayed on the facility websites.

APP 8: CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

PMA may enter into arrangements with third parties to store data we collect, and such data may include personal information, outside of Australia. PMA will take reasonable steps to ensure that the third parties do not breach the APP's. The steps PMA will take may include ensuring the third party is bound by privacy protection obligations which are the same (or substantially the same) as those which bind PMA and requiring that the third party have information security measures approved by PMA.

APP 9: ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

PMA does not use government related identifiers for patients, but uses its own computer-generated unique patient identifiers (Medical Record Numbers) within its facilities. Government related identifiers will not be disclosed unless the use or disclosure is necessary for identification purposes, permitted by law or for the fulfilment of our obligations to an agency or State authority.

APP10: QUALITY OF PERSONAL INFORMATION

PMA will take reasonable steps to ensure that any personal information which we may collect, use or disclose is accurate, complete and up-to-date.

APP 11: SECURITY OF PERSONAL INFORMATION

PMA will take reasonable steps to protect all personal information from misuse, interference, loss, unauthorised access, modification or disclosure. We use technologies and processes such as access control procedures, network firewalls, encryption and physical security to protect privacy.

PMA will destroy or permanently de-identify any information which is in its possession or control and which is no longer needed for the purpose for which it was collected provided PMA is not required under an Australian law or court/tribunal or otherwise to retain the information.

APP 12 & APP13 ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Patients have a right to access the health information that we hold in their health record. Patients can also request an amendment to their health record should they believe that it contains inaccurate information.

PMA will allow access or make the requested changes unless there is a reason under the Privacy Act 1988 (Cth) or other relevant law to refuse such access or refuse to make the requested changes.
If we do not agree to change the medical record/personal information in accordance with a patient's request, we will permit the patient to make a statement of the requested changes and we will enclose this with their record.

Should any patient wish to obtain access to or request changes to their health record they can ask for our Privacy Officer (see details below) who can give more detailed information about PMA's access and correction policy [see IM Policy 1.7 'Request for Access to Information.].

Please note that PMA may recover reasonable costs associated with supplying this information.

If a patient has a complaint about privacy issues

If: (a) a patient has questions or comments about this Privacy Policy;
(b) PMA does not agree to provide access to personal information; or
(c) a patient has a complaint about our information handling practices,
they can lodge a complaint with or contact the Privacy Officer on the details below or directly with the Federal Privacy Commissioner.

How to contact us

1. By letter: Privacy Officer, Presmed Australia, **Suite 503, 35 Grafton Street, Bondi Junction, NSW 2022**
2. By email: rcronin@presmed.com.au
3. By telephone or fax:

Chatswood Private Hospital	Ph: (02) 9413 4822 Fax: (02) 9413 3845
Epping Surgery Centre	Ph: (02) 9868 6555 Fax: (02) 9868 6544
Central Coast Day Hospital	Ph: (02) 4367 3880 Fax: (02) 4367 3881
Laser Vision Clinic Central Coast	Ph: 1300 404 484 Fax: (02) 4367 0055
Madison Day Surgery	Ph: (02) 8445 0633 Fax: (02) 8445 0646
MetWest Eye Centre	Ph: (02) 9622 7667 Fax: (02) 9622 7521
Sydney Pain Day Surgery	Ph: (02 9672 1410)
Devonport Eye Hospital	Ph: (03 6424 6111)

HOW PRESMED HANDLES PERSONAL INFORMATION ACQUIRED VIA OUR WEBSITE

This section of the Privacy Policy explains how we handle personal information which is collected from our websites: www.presmed.com.au, www.eesc.com.au, www.cph.com.au, www.ccdhospital.com.au, www.lvccc.com.au, www.optomonline.com.au, www.madisonds.com.au, www.metwesteyecentre.com.au

This Privacy Policy applies to use of our websites and the use of any of the facilities on our website.

Collection

When people use our website, we do not attempt to identify them as individual users and we will not collect personal information they specifically provide this to us.

Sometimes, we may collect personal information if someone chooses to provide this to us via an online form or by email, for example:

- Completing an Online Preadmission Form
- submitting a general enquiry via our contacts page;
- registering to receive share market reports; or
- sending a written complaint or enquiry to our Privacy Officer.

When people use our website, our Internet Service Provider (ISP) will record and log for statistical purposes the following information about the visit:

- their computer address;
- their top level name (for example, .com,.gov, .org, .au etc);
- the date and time of the visit;
- the pages and documents accessed during the visit; and
- the browser used.

Our web-site management agent may use statistical data collected by our ISP to evaluate the effectiveness of our web-site.

We are, however, obliged to allow law enforcement agencies and other government agencies with relevant legal authority to inspect our ISP logs, if an investigation being conducted warrants such inspection.

Cookies

A "cookie" is a device that allows our server to identify and interact more effectively with a website visitor's computer. Cookies do not identify individual users, but they do identify the user's ISP and browser type.

Presmed Australia's websites use temporary cookies. This means that upon closing the browser, the temporary cookie assigned to the user will be destroyed and no personal information is maintained which will identify them at a later date.

Personal information such as their email address is not collected unless it is provided to us. We do not disclose domain names or aggregate information to third parties other than agents who assist us with this website and who are under obligations of confidentiality. Users can configure their browsers to accept or reject all cookies and to notify them when a cookie is used.

Links to third party websites

We may create links to third party websites. We are not responsible for the content or privacy practices employed by websites that are linked from our website.

Use and disclosure

We will only use personal information collected via our website for the purposes for which this information has been given.

We will not use or disclose personal information to other organisations or any one else unless:

- the user has consented for us to use or disclose their personal information for this purpose;
- the user would reasonably expect or we have told them (including via this policy) that their information is usually used or disclosed to other organisations or persons in this way;
- the use or disclosure is required or authorised by law;
- the use or disclosure will prevent or lessen a serious or imminent threat to somebody's life or health; or
- the disclosure is reasonably necessary for law enforcement functions or for the protection of public revenue.

If we receive a user's email address because they sent us an email message, the email will only be used or disclosed for the purpose for which it was provided and we will not add the email address to an emailing list or disclose this to anyone else unless consent for this purpose is provided.

Data quality

If we collect personal information from our website, we will maintain and update this information as necessary or when we are advised that this personal information has changed.

Data Security

Presmed Australia is committed to protecting the security of all personal information. We use technologies and processes such as access control procedures, network firewalls, encryption and physical security to protect the privacy of information. We will take all reasonable steps to prevent information from loss, misuse or alteration.

If users choose to complete our online forms or lodge enquiries via our website, we will ensure that their contact details are stored on password protected databases.

Staff members associated with website maintenance have access to our website's backend system. This is password protected. Our website service is also password protected.

PresMed facilities use FYDO electronic Patient Administration System (PAS) to access and store patient data and to generate the clinical record. The system is supported by Altura Health.

FYDO DATA SOVEREIGNTY

- All data is stored on Amazon servers located within the SYD data centre
- All data is encrypted at rest and in transit
- The database is backed up every 6 hours
- The documents e.g. imported document & typed letters are backed up once daily
- Backup restoration can be performed within 24 hours
- Backups are stored on Amazon storage servers

FYDO **SECURITY**

- Altura Health engages in regular penetration testing and certification with third party industry experts
- A copy of the most recent security assessment results can be obtained by contacting us via email at support@alturahealth.com.au or by calling 02) 9632 0026

FYDO ACCOUNT ACCESS

- FYDO requires 2 step authentication which can be setup either via email, SMS code or google authenticator
- Each account is given the option to do this each login, or utilise the 'Remember me for 30 days' feature

Access and correction

If someone wishes to obtain information about how to access or correct their personal information collected via our website, they should refer to APP 12 & 13 - Access and Correction, in the above policy.

ATTACHMENT: Document 1.3.1 'Condensed Privacy Information'

REFERENCES:

1. Australian Government Privacy Act 1988
2. Australian Government Privacy Amendment (Enhancing Privacy Protection) Act 2012
3. Australian Government Office of the Australian Information Commissioner '*Privacy Fact Sheet 17:Australian Privacy Principles'*
4. Benchmarked against other Health Care organisations Privacy Policies
5. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme updated 2019 accessed 3/05/2021
6. NSW Private Health Facilities Act 2007
7. NSW Private Health Facilities Regulations 2017
8. NSW Ministry of Health PD2013_033 *'Electronic Information Security Policy – NSW Health'*
9. TAS Health Service Establishments Regulations 2021
10. TAS Health Service Establishments Act 2006

RATIFIED BY:	Quality Review Committee
DATE:	May 2023
REVIEW DATE:	May 2024
PREVIOUS REVIEW:	2009, 2011, 2014, 2016, 2017, 2019, 2021

DATE	POLICY CHANGES
August	• Addition FYDO data sovereignty • Addition references applicable to Tasmania
May 2023	• Updated facilities
May 2022	• Added references to MetWest Eye Centre details

June 2021	• Updated IM 1.4.2 • Additional reference
June 2019	• Updated to specify AMP rather than CMP. • Updated to replace wording “Facility Rules” with “Presmed By-Laws”. • Updated to include actions to be taken to mitigate the risk of emailing patient personal information to an incorrect recipient. • Deleted reference to COFFS • Addition of policy attachment: PD2013_033 Electronic Information Security Policy - NSW Health
September 2017	• Added references to Madison Day Surgery and Coffs Day Hospital details
December 2016	• Amended terminology to replace “you” with third person equivalents. • Added reference to “Online preadmission form”.
May 2014	• Reformatted to suit current polices • Updated name and position in Manual (from 1.10 Privacy Policy Statement) • Updated CMP • Updated References • Updated content in line with the reference documents