LPH-GEN022 Privacy and Confidentiality Policy

STATEMENT:

This policy is about how we manage personal information of individuals. It outlines the kinds of personal information we collect and hold, how we do so and the purposes for which we collect, hold, use and disclose it. This policy also states how individuals may access personal information about them that we hold, how to seek correction of it, how they may complain about any breach by us of privacy laws and how we will deal with any such complaint. This policy also states whether we are likely to disclose personal information to overseas recipients and, where practicable, those recipients' countries.

There may be other communications we have or make relevant to privacy matters, depending on the particular situation. These may, for example, be in separate forms or contract terms.

This privacy policy does not apply to our management of personal information which is not governed by relevant law such as the *Privacy Act* 1988 (Cth) or applicable State privacy laws (for example the *Health Records and Information Privacy Act* 2002 (NSW)). The information set out in this privacy policy is subject to exceptions or qualifications which are provided for in those laws.

Health services are provided at our facilities by health professionals and others who are not our employees. In relation to those services, those providers may also collect, hold, use and disclose some or all of the same personal information as we do. Those health professionals and others may have different policies regarding the management of personal information than us. This privacy policy concerns only our own policies regarding the management of personal information we collect and hold.

For the purpose of this policy, a “patient" means an individual who is receiving, or who has applied for admission to receive, health services at our facilities.

Health information referred to in this policy will generally be of the kind which is appropriate to our integrated medical facilities for health services, ensuring safety at our facilities, managing those facilities effectively and, in the case of our staff and suppliers, for the proper conduct of our relationships. Health information we collect and hold will typically be some or all of the following:

- medical history of an individual and their family, including current health status (for example diagnoses and conditions, medications, allergies, medical and surgical history and vaccination history)
- functional abilities and care needs (mobility, activities of daily living aids, cognitive status, communication abilities, dietary requirements and continence status)
- advance health care directives
- social and psychological well-being (for example mental health history, social interests and preferences, personal lifestyle and support network).

POLICY REFERS TO:

All LPH Staff
VMO’s (CMO’s, Anaesthetists and Surgical Assistants)
Patients
All students, volunteers and contractors

Who are we?

We are Lakeview Private Hospital Pty Ltd ABN 57 154 883 815, and its controlling entities LPH Medical & Solent Trust. Any reference to "we", "our" and "us" is a reference to these entities and those of its related companies in relation to their activities and operations in providing integrated medical facilities for health services, including surgical, radiology, pathology, pharmacy and rehabilitation services.

The kinds of personal information we collect and hold

The kinds of personal information that we collect and hold will depend on the purposes for doing so. Personal information will typically be of the kinds set out in the table below:

Patient personal information	– Name – Date of birth – Address and telephone contact details – Occupation – Health information we consider may be relevant to our patient services – Health fund details – Ethnic background we consider may be relevant to our patient services – Information provided to us with consent to assist our staff in diagnosis and treatment – Representatives', including emergency contacts', name, relationship with patient, address details and telephone numbers – Information concerning financial matters relevant to payment for our services – Preferences regarding communications, including for marketing purposes
Information about health professionals, students and trainees	– Address and telephone contact details – Name of business/company – Credentials relevant to roles at our facilities and services provided – Information identifying dates of attendance at our facilities and services or activities on those dates. – Details of payments by us and to us – Driver licence and vehicle information for vehicle and traffic management purposes
Recruitment and employment information	– Address and telephone contact details – Date of birth – Driver license details – Tax file number – Superannuation details – name, relationship, address details and telephone number of relevant relationships, including emergency contacts – CV, resume or application-related information, for example information about eligibility to work in Australia, education, academic transcripts, employment and criminal histories, professional memberships or trade qualifications – Health information connected with suitability for employment – Background information checks, including references and referees' opinions about work performance as well as any other information that may be provided during background checking processes – Driver licence and vehicle information for vehicle and traffic management purposes

Visitor registers	– Name – Name of business/company – Address and telephone contact details – Date of visit – Purpose of visit – Immunisation details – Driver licence and vehicle information for vehicle and traffic management purposes
Community event information	– Name – Address and telephone contact details – Image, video recordings and audio recordings
CCTV footage	Photographs, images and video recordings.
Public and government sourced information	– Government records such as details from Commonwealth government initiatives for example My Health Records and the Australian Immunisation Register – Information accessible via search services (for example recruitment and company/business name data) – Information which we are authorised or required by law to collect, for example workers compensation information
Information posted on online portals and forums	Information which individuals post on online portals and forums relevant to our business and activities.
Suppliers	– Name – Business/company name – Address and contact details – Information about suppliers' services – Health information where relevant to the purpose of the relevant supplier arrangement – Information for payment transactions such as bank account and payment card details
Other	We may collect other kinds of personal information with an individual's consent or where that collection is within the individual's reasonable expectations.

How we collect personal information

How we collect personal information varies according to an individual's circumstances and the purpose for which we collect the information.
The following sets out the typical sources for our collection of personal information and the typical ways in which we collect it.

Sources

The sources of personal information we collect are mainly from:

- Patients and other individuals directly
- Representatives (for example patients' next of kin and emergency contacts)
- Patients' health professionals, students and trainees who are or may be interacting with patients at our facilities
- Employees and contractors and prospective employees and contractors
- Regulators (including taxation, law enforcement, health, employment and corporate regulators).

Ways of collecting personal information

We typically collect personal information in person, via communications and forms (paper, electronic, online and telephone) and (in the case of CCTV and community events) photography, video recordings and sound recordings.

The typical means for this collection are in the following table:

Directly from individuals	For most of the patient and other personal information we collect, we do so directly from the individuals. This can be in person, via admission forms and patient consent forms and via online interactions (through our website, our apps, by social media and by smartphones and tablets). In the case of some health information, we collect this via observations of individuals and from the use of diagnostic equipment (for example clinical images)
From third parties	We collect personal information from: – Health professionals who are providing services to patients at our facilities – Individuals' representatives (for example patients' next of kin and emergency contacts) – Employers where a health service at our facility is connected with employment – Community/hospital events organisers and participants
Government	We may receive personal information from government agencies, for example about an individual who has been an employee or patient at our facilities
Online sources	We collect some personal information by searching for it, for example using search services for recruitment, social media sites or company/business name search services
CCTV	We place CCTV devices at our facilities for security purposes and so that we may have a record of any incidents occurring at them
Other	We may collect personal information in other ways, where doing so is with an individual's consent or within their reasonable expectations.

How we hold personal information

We hold personal information in paper format at our business sites and in electronic form in systems owned or controlled by us or by a third-party service provider. We have security measures in place regarding third-party hosting of our databases which include personal information.

Purposes: why we collect, hold, use and disclose personal information

We collect personal information from, and disclose personal information to, a variety of people. We usually disclose personal information to such third parties as are reasonably appropriate in connection with our purposes.
Depending on the types of personal information involved, these people are mainly:

- patients
- patients' representatives (for example patients' next of kin and emergency contacts)
- visitors to our facilities
- volunteers at our facilities
- suppliers to patients and to us (including health professionals)
- employees and contractors, and prospective employees and contractors and
- regulators (including taxation, law enforcement, health service, employment and corporate regulators).

Our purposes of collecting, holding, using and disclosing personal information are generally for the effective management of relationships with patients and of our functions and activities in operating and promoting our facilities.

The terms of contracts with us and notices we provide at or around the time of collection (for example patient admission forms) may give additional notice of our purposes.

Some specific purposes are as follows. Not all of these apply to all kinds of personal information we collect and hold, and not all of them apply to those from or to whom we collect or disclose personal information.

- Providing, and facilitating the provision and management of, health services at our facilities
- Communicating with service providers and patient representatives in connection with health services at our facilities
- Complying with laws relevant to our facilities, including laws regulating the provision of health services and health and safety procedures
- Recording, investigating and responding to health or safety incidents
- Assessing and monitoring individuals for paid and unpaid engagements at our facilities
- Drug and other medical screening relevant to services provided at our facilities
- Administering relationships, relevant to our facilities, with past, present and future health professionals, employees, contractors, supervisors, volunteers, trainees and students
- Providing support in respect of technical and professional skills and well-being of those who may have a role at our facilities
- Processing payments for services provided at our facilities
- Enrolling individuals on our mailing lists
- Data analytics, with or without de-identification
- Direct and indirect marketing not involving the use of individuals' sensitive information
- Purposes which are within individuals' reasonable expectations
- Purposes which have been consented to by individuals.

Business acquisitions

From time to time, we may be involved in actual or proposed business acquisitions. For these, we may collect, hold, use and disclose personal information to, with or from third parties (namely counterparties to those transactions).

In these situations, it is our policy to observe the following:

- require confidentiality arrangements to be in place before any personal information transfers;
- only collect or as required disclose personal information to the extent reasonably appropriate, for example appropriate due diligence processes;
- be satisfied about the security arrangements attendant on the transfers of personal information to and from the counterparties;
- de-identify personal information until such time as identification is reasonably necessary and
- have arrangements in place for the destruction or delivery up of personal information to the extent it is no longer reasonably required in connection with the relevant transaction.

Pseudonyms and anonymity

It is generally not practicable for our activities and operations to be carried out in respect of individuals whose identity is not reasonably apparent to us. There are also some laws that require or authorise us to deal with those who have identified themselves. We may decline our services to, and other interactions with, individuals who choose not to identify themselves when dealing with us.

Marketing communications

We communicate details about our activities and services to past, existing and potential clients and their representatives. These communications are sent in various forms, including mail, SMS, email, telephone and social media. Individuals can opt out of receiving direct marketing communications at any time by lodging a request with our Privacy Contact or by using opt out facilities provided in our direct marketing communications. We are required to have individuals' consent to the use or disclosure of their sensitive information (which includes their health information) for the purpose of direct marketing which is the subject of the *Privacy Act* 1988 (Cth).

How individuals may access and seek correction of their personal information

Individuals may request access to personal information we hold about them by making a request by telephone or email to our Privacy Contact. For phone contacts, our Privacy Contact may ask that the request be put in writing. Contact details for our Privacy Contact are set out below. We may charge a fee for providing access if it requires a significant amount of time to locate the requested personal information or to collate or present it in an appropriate form. We may decline to provide access to personal information where doing so may have an unreasonable impact upon the privacy of others or where we are not required by applicable privacy or other laws to give that access.

Where their personal information is inaccurate, out of date, incomplete, irrelevant or misleading, individuals may inform us of this and request that we correct it. We may decline such request where we are not required by applicable privacy or other laws to make such correction.

Complaints

If individuals are not satisfied with how we manage their personal information, they may lodge a complaint in writing with our Privacy Contact. Our policy is to aim for a response time within 14 days to discuss concerns and outline options about how they may be resolved. Our policy is to aim for privacy complaints to be resolved in an appropriate manner with which the complainant is satisfied. Individuals may contact our Privacy Contact to enquire about the progress of their complaint.

If individuals are not happy with how we have resolved their complaint, they may lodge a complaint with the relevant regulator. Under the *Privacy Act* 1988 (Cth) this is:

Australian Information Commissioner
www.oaic.gov.au
Telephone: +61 1300 363 992

Under the *Health Records and Information Privacy Act* 2002 (NSW) this is:
Information and Privacy Commission New South Wales
www.ipc.nsw.gov.au
Email: ipcinfo@ipc.nsw.gov.au
Telephone: 1800 472 679
Address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 or GPO Box 7011, Sydney NSW 2001

Disclosures to overseas recipients

In connection with services

- provided by us via or from a provider who is located, or uses locations outside Australia or
- outsourced by us to a provider who is located or uses locations outside Australia, for example, data storage services,

we are likely to disclose personal information outside Australia. These overseas recipients or their data storage servers may be located, and may store personal information from time to time, in a number of countries.

For practical and security reasons, we are not able to provide a complete list of the organisations and locations to which we share personal information, however the provider of the platform we use for some app-based communications with patients and the storage of some of their personal information uses servers for data storage which are located in the United States of America.

Our privacy contact

Individuals may contact us about privacy matters. Our Privacy Contact's details for this are:
Telephone: *02 8711 0516*
Email: *info@lakeviewprivate.com.au*
Post: *Executive assistant*

Modifications and updates

We may change this privacy policy from time to time. If we do this, we will give 14 days' prior notice of the change by a posting on our website. If an individual does not agree to our continued use of their personal information due to the changes in our Privacy Policy, they may cease providing us with their personal information and contact our Privacy Contact at the details given above.

Information Disclosure and Confidentiality
Information held by Lakeview Private Hospital is confidential and must not be disclosed to a patient's family member, next of kin (NOK), relative, carer or other third party unless the disclosure is authorised by the patient, permitted or required by law, or otherwise constitutes a lawful disclosure. LPH recognises that patient representatives, including NOKs and emergency contacts, may be involved in a patient's care; however, their status as a representative or NOK does not automatically authorise access to all patient information, particularly sensitive health or financial information.
Information may be disclosed where:

- The patient has provided consent to the disclosure.
- Disclosure is necessary for the provision, coordination or ongoing management of health care, where permitted under applicable privacy legislation.
- Disclosure is required or authorised by law, including where required for the administration of relevant health legislation.
- Disclosure is required for legal proceedings, including where authorised by a court order, subpoena or other lawful process.
- Disclosure is necessary to comply with a lawful direction or statutory requirement.
- Disclosure is permitted for certain public health, research or epidemiological purposes, where authorised by legislation and subject to applicable confidentiality requirements.
- Disclosure is otherwise permitted under applicable Commonwealth or NSW privacy and health records legislation.

Financial information is particularly sensitive. Staff must not discuss a patient's account, payment arrangements, health fund information, outstanding balance or other financial matters with a NOK, relative or carer unless the patient has authorised the disclosure or there is another lawful basis for doing so. LPH's Privacy Policy identifies financial information relevant to payment for services as personal information held by the hospital.

Procedure

1. All staff, VMOs, contractors, volunteers and students must maintain the confidentiality of personal and health information accessed in the course of their duties and comply with the LPH Code of Conduct and applicable privacy legislation.
2. A patient's right to privacy and confidentiality must be respected at all times.

3. Staff must not intentionally access, use or disclose patient information except where required or authorised for their employment duties or otherwise permitted by law.
4. Staff must only access information necessary to perform their role and must not access patient records out of curiosity or for personal reasons.
5. All employees, volunteers and students must complete and sign the required privacy and confidentiality declaration on commencement.
6. Patient information must not be disclosed to family members, NOKs, carers or other third parties without appropriate consent or another lawful basis for disclosure. This includes obtaining verbal consent from the patient before bedside clinical handovers or doctors rounds if others are present.
7. Where a patient has nominated a NOK, emergency contact or representative, staff must confirm the extent of the authority provided before disclosing health, personal or financial information.
8. Medical records and other patient information must remain confidential and be securely stored.
9. The Medical Records area must remain locked or appropriately secured when unattended.
10. Where applicable and authorised, health information may be uploaded to or shared through **My Health Record** in accordance with the patient's consent and applicable legislation.
11. It is standard practice to provide the patient's GP and other healthcare providers involved in their ongoing care with relevant discharge information to support continuity of care.
12. Where staff are uncertain whether information can be disclosed, no disclosure should occur until advice has been obtained from the appropriate manager, Privacy Contact or other authorised person.
13. Any suspected privacy breach, unauthorised access or inappropriate disclosure of patient information must be reported in accordance with LPH's incident and privacy breach processes.

EXPECTED OUTCOMES:
LPH will protect the privacy and confidentiality of **patient and staff information**, ensuring personal and health information is only accessed, used or disclosed with appropriate consent or where authorised or required by law. Staff will understand and comply with their confidentiality obligations and promptly report and manage any actual or suspected privacy breaches.

RELATED DOCUMENTS:
LPH-MR001 Access to Medical Records
LPH-HR003 Code of professional conduct
LPH153 Employee Confidentiality agreement
LPH-GEN034 Notifiable Data Breach

REFERENCES:
NSW Privacy Manual for Health Information, 2025
Mental health Act 2007
Public Health Act 2010
NSW Privacy Management Plan Oct 2024
Health Records and Information Privacy Regulation 2022

APPROVAL AND IMPLEMENTATION:
Policy Custodian: Quality Manager
Authorising Committee: CQI

VERSION CONTROL:

Version	Date	Comments
1	2015	New Document
1	2018	Reviewed, nil changes
2	2021	Reviewed, changes made
3	2023	Reviewed, changes made regarding contact NOK
4	2026	Reviewed, major changes – re-type of information collected – reference updated and related documents

Date of next review: September 2029