# PERSONAL DATA PROTECTION POLICY

This Policy is effective as of 10th April 2026.

## 0. Language

This Privacy Policy is provided in both Thai and English. Both versions shall have equal legal effect. In the event of any inconsistency, the provisions shall be interpreted in good faith to reflect the original intent of this Policy.

## 1. Policy Introduction

Pacific Healthcare (Thailand) Co., Ltd. (the "Company" or the "Organization") recognizes the importance of personal data and other information relating to data subjects (collectively, "Data"). To enable data subjects to be confident that the Company maintains transparency and accountability in the collection, use, or disclosure of their personal data in accordance with the Personal Data Protection Act B.E. 2562 (2019) (the "Personal Data Protection Law") and other applicable laws, this Personal Data Protection Policy (the "Policy") is established to explain to data subjects details regarding the collection, use, or disclosure (collectively, "Processing") of personal data carried out by the Company, including by officers and related persons acting for or on behalf of the Company, as set out below.

## 2. Scope of Application

This Policy applies to the personal data of individuals who currently have, or may in the future have, a relationship with the Company, whose personal data is processed by the Company, its officers, employees, contract workers, business units, or other organizational units operated by the Company. This includes contractual partners or external persons who process personal data for or on behalf of the Company ("Personal Data Processors") under various products and services such as websites, systems, applications, documents, or other services supervised by the Company (collectively, the "Services").

Individuals who have a relationship with the Company as described above include:

1) Individual customers;
2) Officers or workers/employees;
3) Business partners and service providers who are individuals;
4) Directors, authorized persons, representatives, agents, shareholders, employees, or other persons having a similar relationship of juristic persons that have a relationship with the Company;

5) Users of the Company's products or Services;
6) Visitors to or users of websites supervised on behalf of the Company, including systems, applications, devices, or other communication channels supervised by the Company; and
7) Other persons whose personal data is collected by the Company, such as job applicants, family members of officers/employees, guarantors, insurance policy beneficiaries, etc.

Items (1) to (7) above are collectively referred to as "Data Subjects".

In addition to this Policy, the Company may issue a privacy notice (a "Notice") for specific products or services to inform data subjects of the personal data processed, the purposes and lawful bases for processing, the retention period, and the personal data rights applicable to that specific product or service. In the event of any material inconsistency between the Notice and this Policy, the relevant Notice for that product or service shall prevail.

## 3. Definitions

- **Company:** means Pacific Healthcare (Thailand) Co., Ltd. and all affiliated companies as listed in the appendix to this Policy.
- **Personal Data:** means any information relating to a natural person that enables the identification of such person, whether directly or indirectly, but excludes data of deceased persons and any other information that does not qualify as personal data.
- **Sensitive Personal Data:** means personal data as prescribed under Section 26 of the Personal Data Protection Act B.E. 2562 (2019), including racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data (used for identification or authentication), or other data which has a similar impact on the data subject as may be announced by the Personal Data Protection Committee.
- **Processing of Personal Data:** means any operation performed on personal data, such as collection, recording, copying, organization, storage, updating, alteration, use, retrieval, disclosure, transmission, dissemination, transfer, combination, erasure, destruction, etc.
- **Data Subject:** means a natural person who is the owner of personal data that the Company collects, uses, or discloses.
- **Data Controller:** means a person or juristic person having the authority to decide on the collection, use, or disclosure of personal data.
- **Data Processor:** means a person or juristic person who processes personal data relating to the collection, use, or disclosure of personal data under the instruction of, or on behalf of, the Data Controller; provided that such person or juristic person is not a Data Controller.

- **Data Protection Officer (DPO):** means a person or a committee appointed by the Company under the Personal Data Protection Act B.E. 2562 (2019) to provide advice, monitor the operations of the Data Controller or Data Processor, coordinate and cooperate with the Office of the Personal Data Protection Committee, and be able to report directly to the highest management of the Data Controller or Data Processor where there are issues relating to the collection, use, or disclosure of personal data.

## 4. Sources of Personal Data Collected by the Company

Personal data collected directly from data subjects through various service channels, such as application, registration, recruitment, contract execution, documentation, surveys, use of products or services, other service channels supervised by the Company, or when data subjects communicate with the Company at the Company's premises or through other supervised contact channels;
Data collected from data subjects' use of the Company's website, products or other services under a contract or mandate, such as tracking usage behavior of the Company's website, products or services through cookies or software on the data subject's device; and
Personal data collected from sources other than the data subject, where such sources have authority, lawful grounds, or have already obtained the data subject's consent (where required) to disclose such data to the Company, such as linkage with government digital services, receiving personal data from government agencies or other third parties where permitted by law (including, where applicable, where the Company is assigned to operate or support a central data exchange), and where necessary to provide services under a contract that may require exchanging personal data with contractual partners.

This also includes cases where a data subject provides the Company with a third party's personal data. In such cases, the data subject is responsible for informing such third party of the details under this Policy or the relevant Notice (as applicable) and obtaining the third party's consent where consent is required for disclosure to the Company.

If a data subject refuses to provide personal data necessary for the Company to provide its services, the Company may be unable to provide such services in whole or in part.

## 5. Lawful Bases for Collecting Personal Data

The Company determines appropriate lawful bases for collecting personal data in accordance with the service context. The lawful bases used by the Company include:

| Lawful basis for collection | Details |
|---|---|
| Performance of a task carried out in the public interest or exercise of official authority, where entrusted to the Company under applicable law | To enable the Company, where applicable, to perform tasks in the public interest or exercise official authority that may be entrusted to the Company under applicable law or mandate, in accordance with the Company's mandate as prescribed by law (e.g., the Digital Government Administration and Services Act B.E. 2562 (2019)), and relevant rules, regulations, orders and Cabinet resolutions. |
| Compliance with a legal obligation | To enable the Company to comply with laws governing the Company, such as the collection of computer traffic data under the Computer Crime Act B.E. 2560 (2017), tax laws, and compliance with court orders, etc. |
| Legitimate interests | For the legitimate interests of the Company and of other persons, where such interests are not less important than the fundamental rights in personal data of data subjects, such as building security or processing personal data for internal business operations. |
| Vital interests | To prevent or suppress danger to life, body, or health, such as providing an application for epidemic surveillance in accordance with government policy. |
| Contractual necessity | To enable the Company to perform obligations under a contract or to take steps at the data subject's request prior to entering into a contract, such as employment, service arrangements, memoranda of understanding, or other forms of contracts. |
| Historical document, research, or significant statistics | To enable the Company to prepare or support the preparation of historical documents, research, or statistics as the Company may be assigned, subject to conditions and appropriate safeguards required by applicable law. |
| Consent | For the collection, use, or disclosure of personal data where the Company is required to obtain consent after informing the data subject of the purposes, such as collecting Sensitive Personal Data (with explicit consent where required) for purposes not within the exemptions under Sections 24 or 26 of the PDPA, or marketing communications about products and services of contractual partners or business allies where consent is required. |

Where the Company needs to collect personal data for contractual performance, legal compliance, or steps prior to entering into a contract, if the data subject refuses to provide personal data or objects to processing for the purposes of such activities, the Company may be unable to perform or provide the service(s) requested by the data subject in whole or in part.

## 6. Types of Personal Data Collected by the Company

The Company may collect or obtain the following information, which may include personal data, depending on the Services used and the relationship context. The categories below represent the general framework for collection. Only data relevant to the specific products or services used or the relationship context shall apply.

| Category of Personal Data | Details and examples |
|---|---|
| Identification data | Information identifying the data subject or information from official documents, such as title, first name, last name, middle name, nickname, signature, national identification number, nationality, driver's license number, passport number, household registration information, professional registration or license numbers, insured person number, social security number, etc. |
| Personal characteristics | Details about the data subject such as date of birth, gender, height, weight, age, marital status, military service status, photographs, spoken language, behavioral data, preferences, bankruptcy status, status as an incompetent person or quasi-incompetent person, etc. |
| Contact information | Information used to contact the data subject such as home telephone number, mobile phone number, fax number, email address, mailing address, online social account identifiers (Line ID, MS Teams), residence location map, etc. |
| Employment and education information | Employment details including work history and education history, such as employment type, occupation, rank, position, duties, expertise, work permit status, references, taxpayer identification number, position history, employment history, salary information, start date, resignation date, benefits and entitlements assessment, assets in possession, work output, bank account number, educational institution, educational qualifications, academic results, graduation date, etc. |
| Service usage information | Details about the Company's products or services such as user account name, password, PIN, Single Sign-On information (SSO ID), OTP, computer traffic data, location data, photographs, videos, audio recordings, usage behavior (websites under the Company's supervision or various applications), search history, cookies or similar technologies, device identifier (Device ID), device type, connection details, browser information, language settings, operating system, etc. |
| Sensitive Personal Data | Sensitive personal data such as race, religion, disability, political opinions, criminal records, biometric data (facial template data), health data, etc. |

## 7. Cookies

The Company collects and uses cookies and similar technologies on websites under the Company's supervision or on the data subject's device (depending on the Services used) for security operations in providing services, and to provide convenience and a good user experience. Such information will be used to improve the Company's website to better meet data subjects' needs. Data subjects may configure or delete cookies through their web browser settings.

If data subjects choose not to accept or to delete cookies, the website may be unable to sell products, provide services, or display content fully and efficiently, and access to and use of certain functions may be slower.

## 8. Personal Data of Minors, Incompetent Persons, and Quasi-Incompetent Persons

Where the Company becomes aware that personal data for which consent is required relates to a minor, an incompetent person, or a quasi-incompetent person, the Company will not collect such personal data until consent has been obtained from a person having parental power acting on behalf of the minor, or a guardian, or a curator, as the case may be, in accordance with legal requirements.

Where the Company was not previously aware that a data subject was a minor, an incompetent person, or a quasi-incompetent person and later discovers that the Company collected such data without having obtained consent from the legal representative, the Company will delete or destroy such personal data as soon as possible if the Company has no other lawful basis apart from consent for the collection, use, or disclosure of such data.

## 9. Purposes of Personal Data Collection

The Company collects personal data for several purposes depending on the type of products, Services, or activities used, and the nature of the relationship with the Company. The purposes below represent the general framework for the Company's use of personal data. Only purposes relevant to the products or Services used, or the relationship context, shall apply.

- To carry out tasks necessary for the public interest assigned to the Company, or as necessary to exercise legal authority under the Company's mandate (where applicable) and applicable laws, rules, regulations or orders;
- To provide and manage the Company's Services, including services under contracts with data subjects or under the Company's mandate (where applicable);
- To carry out the Company's transactions;
- To supervise, use, monitor, inspect and manage Services to facilitate and align with data subjects' needs;

- To retain and improve information relating to data subjects, including documents referencing data subjects;
- To maintain records of personal data processing as required by law;
- To analyze data, including resolving issues relating to the Company's Services;
- To carry out necessary internal management operations, including recruitment, selection of directors or office holders, and qualification assessments;
- To prevent, detect, avoid and investigate fraud, security breaches, prohibited acts or unlawful acts, and potential damage to the Company and data subjects;
- To authenticate and verify identity and information when data subjects apply for or use the Company's Services, contact the Company, or exercise legal rights;
- To improve and develop the quality of products and Services to remain up to date;
- To assess and manage risk;
- To send notifications, confirm orders, communicate and provide updates to data subjects;
- To prepare and deliver relevant and necessary documents or information;
- To verify identity, prevent spam, unauthorized acts or unlawful acts;
- To examine how data subjects access and use the Company's Services, both generally and on an individual basis, and for research and analysis purposes;
- To carry out necessary actions to comply with duties owed to competent regulatory authorities, tax authorities, law enforcement agencies, or other legal obligations of the Company;
- To carry out necessary actions for the legitimate interests of the Company or other persons or other related juristic persons in relation to the Company's operations;
- To prevent or stop danger to life, body or health, including epidemic surveillance;
- To prepare historical documents for the public interest, research, or statistics as assigned to the Company; and
- To comply with applicable laws, notifications, binding orders, or legal proceedings, including processing in relation to court warrants and the exercise of rights relating to data subjects' data.

**10. Categories of Recipients to Whom the Company Discloses Personal Data**

Under the purposes stated above, the Company may disclose personal data to the following recipients. The categories below represent the general framework for disclosure. Only recipients relevant to the products or Services used or the relationship context shall apply.

- Government agencies or competent authorities to whom the Company must disclose personal data for legal compliance or other important purposes (e.g., public interest), law enforcement agencies, regulatory authorities, or other authorities with important purposes, such as the Cabinet, responsible Ministers, Department of Provincial Administration, Revenue Department,

Royal Thai Police, Courts, Office of the Attorney General, Department of Disease Control, Ministry of Digital Economy and Society, Office of the Prime Minister, Department of Consular Affairs, Student Loan Fund, etc.;

- Committees relating to the Company's compliance with applicable laws, where the Company may disclose personal data to committee members (e.g., selection sub-committees, relevant boards, etc.);
- Contractual partners who provide employee welfare services, such as insurers, hospitals, payroll providers, banks, telecom providers, etc.;
- Business allies, such as agencies through which data subjects contact the Company via the Company's Services, marketing service providers, advertising media, financial institutions, platform providers, telecommunications providers, etc.;
- Service providers appointed to provide services for or support the Company's operations, such as data storage providers (e.g., cloud, document warehouse), system/software/application/website developers, document delivery providers, payment providers, internet providers, telephone providers, Digital ID providers, social media providers, risk management providers, external consultants, logistics providers, etc.;
- Other types of recipients, such as persons contacting the Company, family members, non-profit foundations, temples, hospitals, educational institutions or other entities, for purposes such as service operations, training, awards, merit-making, donations, etc.; and
- Public disclosure only where necessary and permitted by law, such as where the Company is required to publish in the Government Gazette or pursuant to Cabinet resolutions, etc.

**11. Sending or Transferring Personal Data to Foreign Countries**

In some cases, the Company may need to send or transfer personal data to foreign countries to achieve service purposes, such as transferring personal data to cloud systems where the platform or servers are located abroad (e.g., Singapore or the United States) to support information technology systems located outside Thailand. This depends on the Services used or the specific activity.

However, as of the effective date of this Policy, the Personal Data Protection Committee had not yet issued an announcement specifying the list of destination countries with adequate personal data protection standards (and may issue such announcements from time to time). Therefore, where the Company needs to send or transfer personal data to a destination country, the Company will implement measures to ensure adequate personal data protection in accordance with international standards, or will proceed under conditions permitting such transfer under the law, including:

- Where the transfer is required by law;
- Where the data subject has been informed and consent has been obtained in cases where the destination country does not have adequate standards, subject to any announcement listing such countries by the Personal Data Protection Committee;
- Where the transfer is necessary for the performance of a contract to which the data subject is a party, or to comply with the data subject's request prior to entering into such contract;
- Where the transfer is necessary for the performance of a contract between the Company and another person or juristic person for the benefit of the data subject;
- Where the transfer is necessary to prevent or suppress danger to life, body or health of the data subject or another person where the data subject is unable to give consent at that time; or
- Where the transfer is necessary for carrying out an important task in the public interest.

**12. Retention Period for Personal Data**

The Company will retain personal data for as long as necessary for the purposes of collection as specified in this Policy, a Notice, or applicable laws. Once the retention period has ended and the personal data is no longer necessary for such purposes, the Company will delete or destroy the personal data, or anonymize it so that it can no longer identify the data subject, in accordance with deletion and destruction standards as announced by relevant authorities or in accordance with international standards.

Nevertheless, in the event of a dispute, the exercise of rights, or legal proceedings relating to personal data, the Company reserves the right to retain such data until the dispute has been resolved by final order or judgment.

**13. Processing by Third Parties / Sub-Processors**

The Company may appoint or engage third parties (data processors) to process personal data for or on behalf of the Company. Such third parties may provide services such as hosting, outsourcing, cloud computing services/providers, or other service arrangements.

Where the Company appoints third parties to process personal data as data processors, the Company will put in place agreements specifying rights and obligations of the Company as data controller and the appointed processor, including the types of personal data, purposes, scope of processing, and other relevant terms. The data processor must process personal data only within the scope specified in the agreement and under the Company's instructions and may not process such data for other purposes.

Where a data processor appoints a sub-processor to process personal data for or on behalf of the data processor, the Company will require the data processor to enter into an agreement with the sub-processor in a form and standard not lower than the agreement between the Company and the data processor.

**14. Personal Data Security Measures**

The Company has measures to protect personal data by restricting access to personal data to specific officers or authorized persons who have a need to access such data for the stated purposes only. Such persons must strictly comply with the Company's personal data protection measures and maintain the confidentiality of personal data obtained in the course of their duties. The Company has organizational and technical security measures that meet international standards and as may be announced by the Personal Data Protection Committee.

In addition, where the Company sends, transfers or discloses personal data to third parties, whether for services under its mandate (where applicable), contracts or other agreements, the Company will impose appropriate security and confidentiality measures as required by law to ensure that personal data collected by the Company remains secure.

**15. Linking to External Websites or Services**

The Company's Services may link to third-party websites or services that may have personal data protection notices with content differing from this Policy. The Company recommends that data subjects review the personal data protection notice of such websites or services before use. The Company has no involvement in, and no control over, the personal data protection measures of such third parties and cannot be responsible for the content, policies, damages, or acts arising from such third-party websites or services.

**16. Data Protection Officer**

The Company has appointed a Data Protection Officer to monitor, supervise and provide advice on the collection, use or disclosure of personal data, including coordination and cooperation with the Office of the Personal Data Protection Committee, in order to comply with the Personal Data Protection Act B.E. 2562 (2019).

**17. Rights of Data Subjects under the Personal Data Protection Act B.E. 2562 (2019)**

The Personal Data Protection Act B.E. 2562 (2019) provides data subjects with several rights. Such rights will become effective when the relevant legal provisions come into force, and are exercisable in accordance with the conditions and limitations prescribed by the PDPA. The details include:

**Right to access:** Data subjects have the right to request access to and obtain a copy of their personal data and to request disclosure of the source of personal data collected by the Company without the data subject's consent, except where the Company is entitled to refuse the request by law or court order, or where exercising such right may affect the rights and freedoms of other persons.

**Right to rectification:** Where personal data is inaccurate, incomplete or not up to date, data subjects have the right to request rectification to ensure the data is accurate, up to date, complete and not misleading.

**Right to erasure/destruction:** Data subjects have the right to request that the Company erase or destroy personal data, or anonymize it so that it can no longer identify the data subject, subject to conditions prescribed by law.

**Right to restriction of processing:** Data subjects have the right to request restriction of the use of personal data in the following cases: (a) during verification of a rectification request; (b) where personal data has been collected, used or disclosed unlawfully; (c) where personal data is no longer necessary for retention but the data subject requests retention for legal claims; or (d) during the Company's verification of lawful grounds or necessity for processing for public interest due to the data subject's objection.

**Right to object:** Data subjects have the right to object to the collection, use or disclosure of their personal data, except where the Company has lawful grounds to refuse the request (e.g., the Company can demonstrate compelling legitimate grounds, or for establishment of legal claims, compliance with or exercise of legal claims, or for public interest).

Right to withdraw consent: Where processing is based on consent (whether given before or after the Personal Data Protection Act B.E. 2562 (2019) becomes effective), data subjects may withdraw consent at any time while the Company retains their personal data, except where the law restricts such right, where the Company is required to retain the personal data, or where processing remains necessary for the performance of a contract between the data subject and the Company that benefits the data subject.

**Right to data portability:** Data subjects have the right to receive their personal data from the Company in a format that is generally readable or usable by automated means and may request the Company to transmit such data to another data controller, subject to conditions prescribed by law.

**18. Complaints to the Competent Authority**

Where a data subject believes that the Company has not complied with the Personal Data Protection Law, the data subject has the right to lodge a complaint with the Personal Data Protection

Committee or any competent supervisory authority appointed by the Personal Data Protection Committee or by law. Prior to lodging such complaint, the Company requests that the data subject contact the Company so that the Company may be informed of the facts and have an opportunity to clarify the relevant issues and address the data subject's concerns at the earliest opportunity.

**19. Amendments to this Policy**

The Company may revise, amend or change this Policy as it deems appropriate and will notify data subjects through the Company's website or other official communication channels. Nevertheless, the Company recommends that data subjects review the updated Policy regularly, especially before disclosing personal data to the Company.

Using the Company's products or Services after the amended Policy becomes effective shall be deemed acknowledgement of the amended Policy. If a data subject does not agree with this Policy, the data subject should stop using the products or Services and contact the Company so that the Company's relevant officers may clarify the facts further.

**20. Contact / Inquiries / Exercise of Rights**

If data subjects have questions, suggestions or concerns regarding the Company's collection, use and disclosure of personal data, or regarding this Policy, or wish to exercise rights under the Personal Data Protection Law, data subjects may contact the Company at:

Pacific Healthcare (Thailand) Co., Ltd.

Website: www.phc.co.th

Email: pdpa@phc.co.th