Privacy Policy

This Privacy Policy is issued by Healthlead Public Company Limited, Icare Health Company Limited, and Healthiness Company Limited (collectively referred to as "the Company").

The Company, along with individuals involved in the collection, use, and disclosure of personal data (collectively referred to as "processing") through various online and offline channels, on behalf of the Company, acknowledges the importance of protecting your personal data and is committed to ensuring the security and protection of such data. The Company will collect, use, and disclose your personal data in accordance with this Privacy Policy, which complies with the Personal Data Protection Act, B.E. 2562 (PDPA) and other related laws.

This Privacy Policy covers various services provided by the Company through websites, social media, and other channels to customers and contacts of the Company. However, it does not apply to employees and job applicants of the Company. By using the Company's services through various channels or providing information to the Company, you agree to the Company's practices as outlined in this Privacy Policy.

1. **Purposes of Personal Data Collection**

1.1 **For Administrative and Management Purposes**
The Company collects personal data to conduct statistical analysis, enhance public relations, and comply with legal and contractual obligations. This includes recording images and audio during meetings, training, and events. The collected data is used to ensure the efficient and lawful operation of our business, including fulfilling contractual commitments, facilitating transactions, and improving the quality of products and services.

With your consent, the Company can leverage your personal data to understand your preferences, anticipate your needs, and offer you more relevant content and promotions.

If you refuse to provide information, the company may be unable to fulfill contractual obligations or provide certain services.

1.2 **For Legitimate Interests of the Company or Others** such as:

- Security measures through CCTV monitoring at all company entrances and store locations.

- Customer relationship management, including handling complaints, satisfaction assessments, employee customer service, and regular communication about our products and services, all designed to benefit you.

- Risk management, including oversight, internal controls, and measures to prevent illegal activities such as fraud and cyber threats.

- Privacy of personal data through measures such as personal data anonymization.

If you refuse to provide information, the company may be unable to provide services effectively.

1.3 **For Your Benefit from using our products and/or services, as you have consented** such as providing you with improved products and services tailored to your needs, offering special promotions, benefits, recommendations, and news, as well as providing opportunities to participate in special events**.**

If you refuse to provide information, the company may be unable to provide services effectively.

2. Sources of Your Personal Data

2.1. Directly from You for example, from information you provided during account registration or membership sign-up; or information you have updated in your account; or information obtained from your interactions with the company or its team; or information related to your purchase or use of the company's products; or from your contact, visits, or searches for products through the company's website, call center, and other channels; as well as information from your participation in various activities, including those on the website, platform, surveys, and seminars

2.2. Tracking Technology when you use the company's website.

2.3. Subsidiaries or affiliated companies

2.4. Third parties such as business partners, social media platforms, and various advertising providers.

This is to ensure that your personal information is up-to-date and to improve the quality and efficiency of our products and services.

3. Stored personal data

- **Personal information** such as name, surname, photo, age, date of birth, gender, national identification number, passport number or other government-issued identification, address, telephone number, email, and LINE ID.

- **Information about internet usage, applications, or other electronic networks** including your browsing history, search history, and interactions with the company’s website, IP address, and other information about the device you use

to access the website, your location while using the website, and data collected from cookies and cookie IDs.

- **Financial information** such as credit/debit card information, credit/debit card number, card type, expiration date, bank account details, and payment history.

- **Transaction information** purchasing behavior, and other information about the products and services you purchase, such as products you have previously purchased and/or used.

- **Audio, visual, or other electronic data that may identify an individual** which may include data related to geographic location.

4. Data Security Measures

4.1. The Company shall implement comprehensive data security measures to protect personal data, including administrative measures, technical measures, and physical measures. Such measures shall include - Access Control: Implementing measures to authorize or restrict access to, use of, disclosure of, and processing of personal data. User Management: Managing user access and assigning responsibilities to prevent unauthorized access, disclosure, or copying of personal data, or theft of devices used to store or process personal data. Audit Trails: Maintaining audit trails to record and track all activities related to personal data, such as access, modification, deletion, or transfer. Security Policy Compliance: Ensuring that all security measures are implemented in accordance with the Company's information security policy, and that they are appropriate to the methods and media used to collect, use, or disclose personal data.

4.2. The Company shall promote awareness and understanding among its employees regarding their obligations and responsibilities in relation to the collection, storage, use, and disclosure of personal data. Such training shall enable the Company to comply with applicable data protection laws and regulations.

5. Data Retention Period

The Company will retain your personal data for the period necessary to fulfill the purposes outlined in this Privacy Policy. For example, if you subscribe to the Company’s newsletter, your data will be stored and used until you unsubscribe or inform us that you no longer wish to receive the newsletter. Furthermore, the Company will retain your computer traffic data for a minimum of ninety (90) days from the date you access the Company’s website. However, the Company will not use such data for analyzing consumption behavior or conducting market research without your explicit consent.

Unless otherwise required or permitted by law, such data may be retained for a period of approximately 5-10 years or for such longer period as may be necessary, such as in accordance with the applicable statute of limitations for the relevant matter, for the purpose of litigation.

6. Disclosure of Your Personal Data to Third Parties

The Company will not disclose your personal data to any third party without your prior consent. However, you acknowledge and agree that, to provide services effectively or to comply with the law, the Company may disclose your personal data to the following parties:

- Affiliated companies
- Business partners
- Data processors located in Thailand
- Government agencies or officials acting in the performance of their official duties

In disclosing Personal Data to such third parties, the Company shall ensure that such third parties maintain the confidentiality of the Personal Data and shall not use the Personal Data for any purpose other than as specified by the Company.

The Personal Data provided by you to the Company shall be stored on a cloud-based data center operated by an external data processor whose servers are located in Thailand. Such transfer of Personal Data to an external data processor is for the purposes of secure storage, data backup, data retrieval, and service provision. The Company has carefully selected and entered into agreements with the relevant service provider regarding appropriate technical and organizational measures to ensure the security of Personal Data and the scope of data processing. By providing your Personal Data to the Company, you consent to the transfer and processing of your Personal Data for the aforementioned purposes.

However, if you believe that the third party to whom the Company has disclosed your personal data has used your personal data for any purpose other than as specified by the Company, you may notify the Company in accordance with the details set out in this Privacy Policy so that the Company may take appropriate action.

Where the Company's services link to third-party websites or services, and such websites or services may have privacy policies that differ from this policy, the Company recommends that you review the privacy policies of such websites or services for more information prior to using them. The Company has no control over and is not responsible for the privacy practices of such third-party websites or services, and cannot be held liable for the content, policies, damages, or actions arising from such third-party websites or services.

In addition, the Company may disclose your personal data to comply with legal obligations, such as disclosing information to government agencies or public authorities. This may also include disclosure in response to lawful requests, such as requests for information in connection with legal proceedings or requests from private entities or other third parties involved in legal processes. Furthermore, the Company may disclose your personal data as reasonably necessary to enforce the Company's terms and conditions. In the event of a corporate restructuring, merger, or sale of the Company's business, the Company may transfer all or part of your personal data that the Company has collected to a related company.

7. Your Right to Control Your Personal Data

7.1. **Correction or deletion of personal data** You may request to correct or delete your personal data at any time. You may request a “Personal Data Subject Rights Request Form” to fill out and submit to the company via dpo@healthleadgroup.com or call: 063-464-0813. Please note that deleting your data may prevent you from receiving our services or may result in a less efficient service.

Upon receipt of a request to delete your personal data from our systems or customer database, we will make every reasonable effort to fulfill your request. However, we may not be able to delete your personal data if: Such deletion would violate the privacy of other users; Such deletion would be unlawful; We are required to retain the data for legal purposes such as litigation or investigations; We are legally required to retain the data; We are required to retain the data for security purposes; or It is technically infeasible to comply with your request.

Please note that even after we have processed your request to delete your personal data, copies of your information may remain on our backup systems or servers. We maintain these backups for disaster recovery and to comply with legal and regulatory requirements.

7.2. **Right of Access** You have the right to request access to and a copy of your personal data in electronic format. You also have the right to request that your personal data be transferred to another party in a machine-readable format. You may also request that we restrict or suspend the processing of your personal data. To exercise these rights, please request a “Personal Data Subject Rights Request Form” by emailing dpo@healthleadgroup.com or calling 063-464-0813.

7.3. **Withdrawal of Consent** You may withdraw your consent given to the company for the processing of your personal data or for specific activities at any time by contacting the company at the details provided below.

If you would prefer not to receive promotional materials and company updates, you may exercise your right to opt out by following these steps:

- If you do not wish to receive information by telephone, please contact dpo@healthleadgroup.com or call 063-464-0813.
- If you do not wish to receive information via email: simply click the "Unsubscribe" link in any email you receive from us.

7.4. **Right to File a Complaint** You have the right to file a complaint with the expert committee under the Personal Data Protection Act if the company or the data processor, including the company's or data processor's employees or contractors, violates or fails to comply with the Act or any regulations issued under the Act.

However, the Company reserves the right to refuse your request in certain circumstances as permitted by law. If the Company decides to refuse your request, you will be informed of the reasons for such refusal. The Company will use its best efforts, including considering technical feasibility, to ensure that you are satisfied with the processing of your personal data. However, if you remain unsatisfied, you may lodge a complaint with the Company or contact the relevant data protection authority.

8. Use of Cookies

The Company employs cookies and other tracking technologies, such as Google Analytics and Facebook Conversion Tracking, to collect data such as browser type, online usage time, pages visited, referring URLs, language settings, and other computer traffic data. These technologies serve various purposes, including enhancing website security, improving user experience, optimizing data presentation, gathering statistical information, and tailoring the website experience to your specific needs while you're online. Moreover, cookies enable us to select and display advertisements or offers that are most relevant to your interests during your online activities or in marketing emails. We also use cookies to track the effectiveness of our online advertising and email marketing campaigns. Please note that we do not use cookies to collect your personal information.

However, most browsers automatically accept cookies. If you do not wish to accept cookies, you may choose to decline or configure your cookie settings. For more information on managing cookies, please visit www.allaboutcookies.org. Additionally, you can find more details about our company's use of cookies in our Cookies Policy.

9. Consent and Withdrawal of Consent in the Case of Minors

When obtaining consent from a minor as the data subject, the data controller must exercise a higher degree of care and apply more stringent standards than those applicable to adults. This is to safeguard minors from deception, fraud, coercion, misrepresentation, or unlawful acts.

9.1 Age Requirements and Nature of Consent

(a) Minors who have not yet reached the age of majority (older than 10 years but not yet legally an adult)

Consent must be obtained explicitly. A minor may provide consent independently only if the legal act concerned is one that the minor must personally undertake, is appropriate for their status and necessary for their livelihood, is solely for acquiring a specific right, or is intended to relieve them from an obligation. In all other circumstances, consent must be obtained from the legal guardian who has the authority to act on behalf of the minor.

(b) Minors aged 10 years or younger

The data controller must obtain consent exclusively from the minor's legal guardian. Consent may not be obtained from the minor directly without the explicit consent of the legal guardian. The process of obtaining consent should include appropriate verification measures, proportionate to the level of risk, to ensure that the individual providing consent is indeed the authorized legal guardian. Additionally, the language and method used must be clear and easily comprehensible to the legal guardian.

9.2 Measures for Verifying the Age of a Minor

The data controller must implement appropriate identity verification measures for the minor or their legal guardian, proportionate to the level of risk involved. The data controller must take into account the impact of collecting, using, or disclosing the minor's personal data as a primary consideration.

9.3 Withdrawal of Consent by a Minor

The principles governing the withdrawal of consent for general data subjects shall apply mutatis mutandis to minors or their legal guardians acting on their behalf.

9.4 Consent and Withdrawal of Consent for Persons Lacking Legal Capacity or Quasi-Incompetent Persons

In cases where the data subject is a person lacking legal capacity or a quasi-incompetent person, consent must be obtained from the guardian authorized to act on behalf of the legally incapacitated person or from the curator authorized to act on behalf of the quasi-incompetent person, as applicable. The principles governing consent under this regulation shall apply mutatis mutandis.

10. Company Information and Data Protection Officer

To ensure effective compliance with our privacy policy, we have appointed a Data Protection Officer who can assist you with any inquiries regarding the management of your personal data. If you have any questions or suggestions about our data handling practices, please contact us at:

HEALTHLEAD PUBLIC COMPANY LIMITED
99/4 Moo 10, Bang Muang, Bang Yai, Nonthaburi 11140

Data Protection Officer
E-mail : dpo@healthleadgroup.com
Tel : +66 63-464-0813