**Fullerton Health Privacy Statement**

**Last updated:** January 2026

We, The Vascular & General Surgery Centre, as part of the Fullerton Health Group, are committed to safeguarding your privacy. We will only use your personal data in the manner set out in this Privacy Statement. This Privacy Statement applies to all personal data that you provide to us and the personal data we hold about you. This Privacy Statement describes how we may collect, use, disclose, process and manage your personal data. Please DO NOT provide any personal data to us if you do not accept this Privacy Statement.

All references to the "Fullerton Health Group", "we", "us" and "our" refer collectively to the Fullerton Health Pte. Ltd. and all its subsidiaries and related companies.

Please note that we also act on behalf of and under the instructions of insurers and other partners that act as data controllers, including for the processing of your health information and health benefits claims. Please refer to their respective privacy policies for more information regarding the processing of your personal data in these contexts.

Indonesia, Philippines, and Vietnam residents, please see our additional Jurisdiction-Specific Terms. If there is any inconsistency between the main terms of the Privacy Statement and the Jurisdiction-Specific Terms, the Jurisdiction-Specific Terms shall prevail.

## AMENDMENT TO THIS PRIVACY STATEMENT

We may amend this Privacy Statement from time to time. To the extent required by applicable law, we will notify you of any changes made to this Privacy Statement before they are implemented. The updated Privacy Statement will supersede earlier versions and will apply to personal data provided to us previously. The updated Privacy Statement will be made available upon request from our Data Protection Officer and on our website at https://www.tvgsc.sg/. If you do not accept any amendment to the Privacy Statement, please contact our Data Protection Officer (refer to section on "Your Rights").

## PERSONAL DATA WE MAY COLLECT

For the purposes of this Privacy Statement, "personal data" is data, whether true or not, about a natural person who can be identified from that data or from that data and other information to which we have or are likely to have access.

Depending on the nature of your interaction with us, the personal data that we collect or process may fall into the following categories:

- General personal data such as name, address, contact details and email address including those of family members;
- Identifiers including unique identification issued by government, insurer or employers;
- Health information such as health and medical records, medical history, diagnoses, sexual life and procedures or test outcomes;
- Job application information when you apply for a job with us, such as education background, employment history and references; and

- Information on IP address, device and mobile app usage, including information collected via cookies and similar technologies.

Based on applicable laws and the nature of your interaction with us, some of the above personal data may be defined as special or sensitive personal data (or an equivalent category under applicable laws in your jurisdiction). In such cases, we will implement appropriate technical and organisational measures to protect its security, confidentiality, and integrity, and comply with any specific processing requirements under the applicable law of your jurisdiction.

Voluntary provision of personal data. Your provision of personal data to us is voluntary. However, if you choose not to provide us with the personal data we require, it may not be possible for us to contact you or provide products or services which you need from us.

Providing the personal data of others. If you provide the personal data of anyone other than yourself (including your family members, employees or insured members – in the case of corporate healthcare arrangements), you warrant that you have informed him/her of the purposes for which we are collecting his/her personal data and that he/she has consented to your disclosure of his/her personal data to us for those purposes.

Accuracy and completeness of personal data. You confirm that all personal data that you provide to us is accurate, complete and up-to-date.

Child Data. We may collect and process the personal data of children, with "child" defined in accordance with applicable law in your jurisdiction. Where required by applicable law, we will obtain verifiable consent from a parent or legal guardian before collecting or processing a child's personal data. If you are a parent or guardian providing us with your child's personal data, you represent that you have the authority to do so and, where relevant, you provide consent to the processing of that data in accordance with this Privacy Statement. If we learn that we have collected a child's personal data without verification of parental consent, we will delete the data. If you believe we might have any personal data from or about a child without your consent, please contact our Data Protection Officer.

**COLLECTION OF PERSONAL DATA**

Generally, we may collect your personal data (at all times in accordance with applicable law) when you or someone whom you authorise, including your employer or insurer:

- register for or use any services or products we provide;
- respond to or register for any of our initiatives or events;
- visit our website;
- send us an email;
- request to be included in our mailing list;
- interact with us, for example, via telephone calls (which may be recorded), letters, face-to-face meetings, social media platforms and emails;
- call us to fix an appointment and/or request that we contact you;

- when your images are captured by us via CCTV cameras while you are within our premises, or via photographs or videos taken by us or our representatives or service providers when you attend our events;

- submit an application for employment, internship or attachment; and/or

- submit your personal data to us for any other reason.

**HOW WE MAY USE YOUR PERSONAL DATA**

We collect, use or disclose your personal data (or, where you are our corporate customer, the personal data of your employees) for the following purposes:

- to manage your relationship with us;

- to provide you with the services that you have requested;

- providing you with customer service and support;

- verifying your identity;

- to administer medical care and related services, including dispensing medication and treatment, liaising with third-party healthcare professionals, clinics, hospitals and/or medical institutions in relation to your medical care (including by providing them with access to your medical records);

- HMO/TPA membership administration, to deliver member benefits to you and your plan sponsor, such as processing your reimbursement requests; intermediating in the administration of medical care, liaising with third-party specialist doctors, clinics, hospitals, and/or medical institutions in relation to your medical care (including by providing them with access to your medical records);

- to assist you with your enquiries;

- to contact you for feedback after the provision of our services;

- to improve our understanding of your interests and preferences, our service quality, to enhance operational efficiency, or to conduct market research;

- and/or purposes which are reasonably related to the aforesaid.

In addition to the purposes set out above, we may also collect, use and/or disclose your personal data for purposes connected or relevant to our business, such as:

- complying with our legal obligations and requirements;

- enforcing obligations owed to us and administering debt recovery and debt management;

- operating, evaluating, developing and improving our products and services;

- finance and accounting, internal controls, risk management and record keeping;
- actuarial and pricing exercise for our HMO products;
- providing your HMO utilisation information to your plan sponsor, subject to applicable law;
- carrying out planning and statistical analysis;
- processing and handling of medical and insurance claims and payments; and staff training;
- monitoring or recording phone calls and customer-facing interactions for quality assurance, employee training and performance evaluation;
- preventing, detecting and investigating crime and analysing and managing commercial risks;
- in connection with any claims, actions or proceedings (including but not limited to drafting and reviewing documents, transaction documentation, obtaining legal advice, and facilitating dispute resolution), and/or protecting and enforcing our contractual and legal rights and obligations;
- managing the safety and security of our premises and services (including but not limited to carrying out CCTV surveillance and conducting security clearances);
- conducting audits or any form of investigations including but not related to those relating to disputes, billing, fraud, offences, prosecutions;
- meeting or complying with any applicable rules, laws, regulations, codes of practice or guidelines issued by any legal or regulatory bodies which are binding on us (including but not limited to responding to regulatory complaints, disclosing to legal, judicial and regulatory bodies and conducting audit checks, due diligence and investigations);
- facilitating business asset transactions (which may extend to any mergers, acquisitions or asset sales); and/or
- purposes which are reasonably related to the aforesaid.

Vendors. If you are an employee, officer or owner of an external service provider or vendor , in addition to the other purposes set out in this Privacy Statement (as may be applicable), we may also collect, use and/or disclose your personal data and/or personal data submitted by you to us for the following purposes:

- assessing your organisation's suitability as an external service provider or vendor for us;
- managing project tenders and quotations, processing orders or managing the supply of goods and services;
- creating and maintaining profiles of our service providers and vendors in our system database;
- processing and payment of vendor invoices and bills;

- facilities management (including but not limited to issuing visitor access passes and facilitating security clearance); and/or

- purposes which are reasonably related to the aforesaid.

Marketing purposes. Where we request for your consent to send you marketing materials and you have opted-in or expressly consented to this request, we may collect, use and/or disclose your personal data for the purposes of marketing our products and services and those of our strategic partners and business associates e.g. informing you of our latest events and services. In order for us to market products and services which are of special interest and relevance to you and in order to collect, use and/or disclose your personal data for these marketing purposes, we may analyse and rely on your overall interaction with us (such as but not limited to your medical and treatment history as well as your other interactions with us).

Withdrawal of consent for marketing purposes. If you have provided us with marketing consent, you have a choice to withdraw your consent using the withdrawal feature or contact details found in our marketing or promotional materials/communication. It may take up to 30 calendar days for your withdrawal to be reflected in our systems, or such other period as may be required under applicable law. Therefore, you may still receive marketing or promotional materials/communication during this period of time. Please note that a withdrawal of marketing consent does not affect the consent you have given for the use of your personal data in relation to the services that you have requested or purchased from us.

Contacting you. When using your personal data to contact you for any of the above purposes, we may contact you via regular mail, e-mail, SMS, telephone or any other means. In relation to the sending of marketing or promotional information, we will only send you such information via regular mail, e-mail, SMS, telephone or any other means where this is permitted under applicable law.

**WEBSITE**

Use of cookies. We may make use of “cookies” on our websites to store and track information such as the number of users and their frequency of use, profiles of users, location and their online preferences. Cookies alone do not capture information which would personally identify you, but the information collected may be used to assist us in providing location-based services such as nearby clinics, analysing the usage of our websites and to improve your online experience with us. If you disable the cookies on our website, this may affect the functionality of our website.

Links to other websites. Our websites may contain links to other websites which are not owned or maintained by us and over which we have no control. These links are provided only for your convenience. When visiting these third-party websites, you do so at your own risk and you should read their privacy policies. You should conduct whatever investigation you feel necessary or appropriate before proceeding with any online or offline transaction with any of these third parties.

**DISCLOSURE OF PERSONAL DATA**

We will not sell your personal data to third parties. Where required and subject to the provisions of any applicable law, your personal data may be disclosed, for the purposes listed above (where applicable) to the following entities or parties, whether they are located overseas or in the territory you are located in:

- between and amongst Fullerton Healthcare Group entities;
- agents, contractors, third-party service providers and network partners (including lab or clinical testing providers, medical appointment-booking providers, and accredited or panel healthcare providers such as clinics and hospitals that support the delivery of our services), and business partners providing services such as hosting and maintenance services, analysis services, e-mail messaging services, delivery services, handling of payment transactions;
- our consultants and professional advisers (such as accountants, lawyers, auditors);
- any business partner, investor, assignee or transferee (actual or prospective) to facilitate business asset transactions (which may extend to any merger, acquisition or asset sale);
- external banks, credit card companies, other financial institutions and their respective service providers;
- relevant government ministries, regulators, statutory boards or authorities or law enforcement agencies to comply with any laws, rules, guidelines and regulations or schemes imposed by any governmental authority (including the Ministry of Health), or any other party to whom we are required or permitted to disclose personal data at law; and/or
- any other party to whom you authorise us to disclose your personal data.

**OVERSEAS TRANSFER OF PERSONAL DATA**

Fullerton Health Group is a regional organisation and personal data we collect will primarily be processed in the locations where we have operations in, including Singapore, Vietnam, Philippines, Hong Kong, Indonesia, Malaysia, and Papua New Guinea. However, we may from time-to-time work with agents, contractors, third-party service providers and business partners which may be based or which undertake business operations outside of these locations. Further, being a cross-border organisation, it is inevitable that there will be certain cases that require international transfers of personal data to countries or territories outside of the jurisdiction you are located in.

If we transfer your personal data to a country or territory outside the one you are located in, we will ensure that such transfers comply with applicable laws, for example by ensuring that the recipient of the personal data provides a comparable standard of protection.

**RETENTION**

Personal data is retained for as long as we have an ongoing legitimate business or legal need to do so – for example, to provide services to you, or as required or permitted by applicable laws, such as tax and accounting laws.

When we have no ongoing legitimate business or legal need to process your personal information, we will either delete or anonymise it.

**SECURITY**

We implement appropriate technical and organisational measures to prevent unauthorised access to personal data, to maintain data accuracy and to ensure the correct use of the personal data we hold. In addition, we limit access to personal data to those employees, personnel, contractors, and other third parties who have a business need to access it. They will only process your personal data on our instructions.

**YOUR RIGHTS**

Data subject rights. You may have certain rights under applicable law to request us for access to, correction of and/or deletion of your personal data in our possession and control. To the extent these rights are available to you under applicable law, you may exercise them in accordance with the details provided in this section.

We reserve the right to refuse your requests for access to, correction of or deletion of, some or all of your personal data in our possession and control if permitted or required under applicable law. This may include circumstances where the personal data may contain references to other individuals or where the request for access or correction is for reasons which we reasonable consider to be trivial, frivolous or vexatious.

Contact Data Protection Officer. If you wish to exercise your data subject rights under applicable law, please contact our Data Protection Officer:

Singapore: dpo@fullertonhealth.com

Fee for access. Subject to applicable law, we may charge you a fee for responding to your request for access to your personal data held by us, or for information about the ways in which we have (or may have) used your personal data in the one-year period preceding your request. If a fee is to be charged, we will inform you of the amount beforehand and respond to your request after payment is received. Subject to applicable law, we will endeavour to respond to your request within 30 days, and if that is not possible, we will inform you of the time by which we will respond to you.

Please note that if your personal data has been provided to us by a third party (e.g. a general practitioner or your employer), you should contact that organisation or individual to make such queries, complaints, and access and correction requests to us on your behalf.

Effect of withdrawal of consent. In many circumstances, we need to use your personal data in order for us to provide you with products or services which you require. If you do not provide us with the required personal data, or if you withdraw your consent to our use and/or disclosure of your personal data for these purposes, it may not be possible for us to continue to serve you or provide you with the products and services that you require.

## LANGUAGE

This Privacy Statement may be translated into one or more other languages. If there is any inconsistency between the English version of this Privacy Statement and other language versions, the English version shall prevail.

## JURISDICTION-SPECIFC TERMS

### Indonesia

If the Indonesian Personal Data Protection Law (Law No. 27 of 2022) applies to your personal data that is processed by us, the following terms apply:

#### COLLECTION OF PERSONAL DATA

The legal bases we rely on to process data. The legal basis on which we process your Personal Data under this Privacy Statement will depend on the type of Personal Data and the specific purposes for which it is collected. Our processing of your personal may be based upon (i) our legitimate interests; (ii) compliance with our legal obligations; (iii) consent you may have provided to us; (iv) and/or any other legal bases under the applicable laws and regulations.

#### YOUR RIGHTS

You may request that we fulfil your rights under the applicable law, such as to:

(i) access and receive a copy of your Personal Data held by us;

(ii) rectify any incorrect Personal Data we might hold about you;

(iii) suspend the processing of your Personal Data in certain circumstances, such as when you request verification of its accuracy, or if you believe our use of your data is unlawful but prefer that the data not be deleted;

(iv) transfer of your Personal Data to you or to a third party in a structured, commonly used, and machine-readable format;

(v) withdraw your consent for certain processing purposes;

(vi) not to be subject to a decision based on automated processing that has legal consequences or significant impact on you, as defined under applicable laws and regulations;

(vii) file a lawsuit and seek compensation for our negligence and/or errors in processing your personal data; and

(viii) erase and dispose of your personal data that we have collected on our server.

The fulfilment of the above rights will be made in accordance with the applicable law.

### Philippines

If you are a resident of the Philippines, the following also applies to you:

**YOUR RIGHTS**

As a data subject, you have the right to lodge a complaint before the Philippine National Privacy Commission.

**Vietnam**

If the personal data protection laws of Vietnam are applicable to our processing of your personal data, the following terms also apply:

**PERSONAL DATA**

You acknowledge that your medical history that we collect is sensitive personal data. We are committed to protecting this information and will implement appropriate technical and organisational measures to ensure its security, confidentiality, and integrity, in compliance with Vietnamese applicable law.

**YOUR RIGHTS**

You have rights in relation to your personal data collected by us, in accordance with Vietnamese applicable law. These rights include the right to be informed about data processing activities, the right to consent or withdraw your consent, the right to access and request correction of your data, the right to request deletion, the right to restrict processing, the right to request provision of your personal data, the right to object to our processing activities, and the right to lodge complaints, denunciations, or initiate legal proceedings and claim compensation, and exercise self-protection in accordance with Vietnamese applicable law.

**SECURITY**

We take steps to ensure that your information is processed securely and in accordance with this Privacy Statement and Vietnamese applicable law. However, you should note that the processing of personal data, including through the internet, carries potential risks, including the risk of unauthorized access, loss, theft, alteration, destruction, or disclosure of such personal data which could lead to undesirable outcomes for you.