

Privacy Policy

Beacon is committed to protecting the rights and privacy of individuals in accordance with the Singapore Personal Data Protection Act 2012 (the “PDPA”).

This policy (“Privacy Policy”) describes how we may collect, use, disclose, process and manage your Personal Data in the course of our business, including our websites, digital services and products such as mobile applications, technical platforms, and other online or offline offerings otherwise indicated. This Privacy Policy applies to any individual’s Personal Data which is in our possession or under our control.

By interacting with us and submitting your data to us, you agree and consent to Beacon as well as our respective agents, authorised service providers and relevant third parties to processing your Personal Data in the manner set forth in this Privacy Policy. If you have any queries related to this Privacy Policy, please contact the persons identified at the end of this Privacy Policy.

This Privacy Policy supplements but does not supersede nor replace any other consents which you may have previously provided to us nor does it affect any rights that we may have at law in connection with the collection, use and/or disclosure of your Personal Data. We may from time to time update this Privacy Policy to ensure that this Privacy Policy is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. As and when the contents of this Privacy Policy are updated or amended, the changes will be uploaded on to our website at <https://beacon.com.sg/apps/bpmc/privacy-policy.pdf>. Each time you use our websites and/or mobile and web-based applications, and any updates, upgrades, new versions, documentation and content and services provided by or through the websites and/or mobile and web-based applications, or contact, interact or transact with us, you acknowledge and agree that the latest version of this Privacy Policy shall apply. It is your duty to keep yourself updated as to the latest version of this Privacy Policy.

This Privacy Policy was last updated on 12 February 2023.

1. Your / Another Person's Personal Data

1.1.

Personal Data” refers to any data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access. For example, “Mr ABC, 40 years old, talent acquisition manager, lives at 12 Ang Mo Kio Central 3” could constitute data that falls under (b).

1.2.

The definition does not extend to (a) business contact information; (b) personal data about an individual that is contained in a record that has been in existence for at least 100 years; (c) personal data about a deceased individual who has been dead for more than 10 years; or (d)

anonymised data. Anonymisation is the process of removing identifying information such that the remaining data does not identify any particular individual.

1.3.

The exact type of personal Data that may apply in your case will vary depending on how you have interacted with us. Some examples of such Personal Data you may provide to us include:

(a)

Personal details (e.g. name, NRIC, FIN, passport or other identification number, contact details, residential address, personal email address, nationality, medical history and background, and/or income levels);

(b)

images and biometrics (e.g. photographs, voice and video recordings of you, including our conversations with you, using fingerprint mapping and facial recognition for verification or other purposes);

(c)

your personal opinions made known to us (e.g. through feedback or surveys); and

(d)

other electronic data or information relating to you through your usage of our products and services or as part of their delivery to you (e.g. location data, IP address, activity logs, cookies, device carrier/operating system and connection type).

1.4.

Any reference to “Personal Data” also includes such data that may be provided by you on behalf of another person pursuant to Clause 3 below.

1.5.

References to “includes,” “including,” “including but not limited to,” “including without limitation” and words or phrases of similar import shall be deemed to have the same meaning and the words “includes(s)” and “including” shall not be deemed to be terms of limitation but rather be deemed to be followed by the words “without limitation”.

1.6.

In relation to Personal Data, “processing” refers to the carrying out of any operations or set of operations on the Personal Data and including any collecting, recording, holding, storing, adaptation or alteration, retrieval, combination, transmission, erasure or destruction of Personal Data.

2. Use and Collection of Personal Data

2.1.

Beacon may use your Personal Data (a) for the purposes identified below or separately communicated to you; (b) to fulfil legitimate business interests and/or contractual and legal obligations; and (c) to comply with applicable laws, regulations and/or requirements from government agencies, regulatory bodies, statutory boards or other relevant bodies in Singapore.

2.2.

Generally, Beacon may collect your Personal Data in the following ways:

(a)

when you submit forms, applications, requests or feedback to us;

(b)

when you enter into any agreement or provide other documentation or information in respect of your interactions with us, or when you use our services;

(c)

when you interact with our customer service officers, for example, via telephone calls, letters, face-to-face meetings, social media platforms and/or emails;

(d)

when you use our electronic services, mobile and web-based applications or interact with us via any of our websites or mobile or web-based applications or use the services on any of our websites or mobile or web-based applications which may utilise various technologies to collect data (which may include Personal Data) automatically either by us or by third parties on behalf of us;

(e)

when you respond to our request(s) for additional Personal Data;

(f)

when we receive your Personal Data from referral parties, government ministries or agencies, regulators, statutory boards, Public Healthcare Institutions, public agencies, your employer and/or other third parties;

(g)

when you attend or participate in our events or activities (e.g. public forums or events) and your voice and/or image data is captured on cameras, audio and/or video recordings;

(h)

when you respond to our initiatives;

(i)

from third parties, including social networks (such as Facebook, LinkedIn or YouTube), when you consent to such third parties disclosing information about you to us that those third parties have collected, whether by logging into or through the social plug-ins on our websites or mobile or web-based applications or otherwise; and

(j)

when you submit your Personal Data to us for any other reason.

2.3.

As a website or app, Beacon may also use some of the following technologies in the services and functionalities in the app. Examples of some of the technologies which may be used (either by us or by third parties on behalf of us) by or in our electronic services, websites and mobile and web-based applications to collect, use and/or disclose Personal Data include the following:

(a)

Authentication confirmations from biometric data services. We do not store biometric data, but may interface with third party biometric data services (such as SingPass which uses biometric-enabled authentication processes for user login) to authenticate your identity when you seek to access BPMCCAMP's services.

(b)

Click-stream data. A visit to one of our websites or use of our mobile or web-based applications result in data that is transmitted from your browser to our server being automatically collected and stored by us or by third parties on behalf of us. This data can include the following:

(i)

the visitor's IP address;

(ii)

the date and time of the visit;

(iii)

the referral URL (the site from which the visitor has come);

(iv)

the pages visited and action taken on our website or mobile or web-based applications; and

(v)

information about the device, mobile carrier and browser used (browser type and version, operating system, etc).

(c)

Cookies. A number of places on our website and our mobile and web-based applications make use of cookies. Should you wish to disable the cookies associated with these technologies, you may do so by changing the setting on your browser. However, you may not be able to enter certain part(s) of our website or enjoy full access to all of our applications.

(d)

Web beacons and tracking links. Web beacons (also known as pixel tags and clear GIFs) involve graphics that are not apparent to the user. Tracking links and/or similar technologies consist of a few lines of programming code and can be embedded in our emails, website or mobile or web-based applications. In conjunction with cookies, these are primarily used for statistical analysis purposes. This technology can also be used for tracking traffic patterns on websites, as well as finding out if an e-mail has been received and opened and to see if there has been any response.

(e)

Web analytics. Web analytics is the term given to a method for collecting and assessing the behaviour of visitors to websites and mobile or web-based applications. This includes the analysis of traffic patterns in order, for example, to determine the frequency of visits to certain parts of a website or mobile or web-based application, or to find out what information and services our visitors are most interested in. For these purposes, we primarily make use of click-stream data and the other techniques listed above. Web analytics are carried out by the Content Management Systems, Google Analytics and/or other selected parties (as we may inform you from time to time) ("**Web Analytics Providers**"). When you visit our website or use any mobile or web-based applications, Personal Data may (unless you have refused the processing of your Personal Data via such cookies and technologies) be sent to the Web Analytics Providers for analysis for and on behalf of us for the purposes described in this Privacy Policy. Please note that if you have created an online profile at our website or mobile or web-based application and if you are logged in on this profile, a unique number identifying this profile may also be sent to the Web Analytics Providers in order to be able to match the web analytics data to this profile. If you do not wish information about your behaviour at our website or any mobile or web-based applications to be collected and assessed by Google Analytics, you can install the Google Analytics opt-out browser add-on. Please refer to Google Analytics Opt-out Browser Add-on page for more information on downloading the add-on and opting out.

(f)

Unique application numbers. Certain services include a unique application number. This number and information about your installation of the application (for example, the operating

system type and application version number) may be sent to us when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

(g)

Local Storage. We may collect and store information (including Personal Data) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches. Such information may include your self-added medication list and medication reminders.

(h)

Retargeting Technologies. Our website and mobile or web-based applications may use retargeting technologies within the Internet. Retargeting technologies analyse your cookies and past surfing behaviour, including clicking of advertisements, so that where you have visited our website, used our mobile or web-based applications or clicked on our advertisements before, we can serve you our advertisements on our partner websites. We may also work with Web Analytics Providers, who use tracking technologies to serve our advertisements to you across the Internet. In order to serve such advertisements, these companies may collect information about your visits to our websites or mobile or web-based applications and your interactions with us and our advertisements. Please refer to our Web Analytics Providers' privacy policy(ies) for more information about their data protection practices. If you do not wish to receive such advertisements, you may adjust your browser settings for the cookies which your browser accepts.

3. Accessing the Personal Data of Others on BPMCCAMP App

3.1.

You may give authorisation to your caregiver to use BPMC App to access your Personal Data. To do so, you will need to provide your National Identification Number (NRIC / FIN / Passport) ("NIN"), as well as the caregiver's NIN, name, email and contact number. Additionally, if you are a parent, you may also apply to access your child's Personal Data if your child is a minor (under 21 years of age). Where so, by applying to obtain or to grant such access, you represent to us that:

(a)

you are authorised to do so;

(b)

you have obtained the consent of the third party to provide us with his/her Personal Data for the respective purposes;

(c)

he/she accepts that his/her Personal Data will be subject to this Privacy Policy (as amended from time to time); and

(d)

you agree to fully indemnify us in respect of any regulatory penalties, claims or proceedings by any third party(ies) and any proceedings, investigations, orders, directions, judgments issued by a court, statutory body or regulatory authority, in connection with the provision of his/her/their Personal Data.

3.2.

You should ensure that all Personal Data submitted to us is complete, accurate, true and correct. Failure on your part to do so may result in our inability to provide you with the products and services you have requested or process your application.

Purposes Related to Your Use of Personal Data on BPMCCAMP

3.3.

Generally, BPMCCAMP App may collect, use and/or disclose your Personal Data for the following purposes:

(a)

setting up your account with us and managing your use and access of BPMCCAMP;

(b)

facilitating your use of our online and mobile services such as the healthcare management programmes and/or the transactional e-services like e-appointments and e-payments;

(c)

managing your relationship with us by personalising our services and recommending content related to your health and our services and informing you about service upgrades and updates;

(d)

carrying out security and safety measures and services such as performing network or service enhancement and protecting our platforms from unauthorised access or use;

(e)

carrying out market-related, evaluation or similar research and analysis for our operational strategy and policy planning purposes, including providing data to authorised external parties for any purposes to review, develop and improve the quality of healthcare products and services;

(f)

verifying your identity and such other information provided by you, including but not limited to the relationship between yourself and a third party dependent or the relationship between yourself and a third party caregiver;

(g)

managing the administrative and business operations more effectively such as attending to your queries, feedback and/or complaints and complying with our internal record keeping for meeting any applicable laws and regulations;

(h)

facilitating business asset transactions (which may extend to any mergers, acquisitions or asset sales);

(i)

carrying out due diligence in accordance with legal and regulatory obligations or our risk management procedures and policies such as conducting audits to prevent, detect and investigate crime or offences or uncover non-conforming processes;

(j)

monitoring or recording phone calls and customer-facing interactions for quality assurance, and identity verification purposes;

(k)

in connection with any claims, actions or proceedings (including but not limited to the drafting and reviewing of documents, transaction documentation, obtaining legal advice, and facilitating dispute resolution), and/or protecting and enforcing our contractual and legal rights and obligations;

(l)

with consents specifically obtained through (or in connection with) national systems such as MyInfo, collecting your profile to compile demographics, user preferences (e.g. likes, topics of interests) and other Personal Data to facilitate your future / further requests in BPMCCAMP and increase your ease of use of BPMCCAMP;

(m)

(where necessary) sending a personalised notification to you in relation to your login and use of BPMCCAMP whether this is in-app or (where you consent) for your usage of other apps connected with BPMCCAMP;

(o)

complying with any request or direction of any government authority or public agencies, ministries, statutory boards or similar authorities or non-governmental agencies authorised to carry out specific Government services and duties; and

(p)

any other purpose reasonably related to the aforesaid.

3.4.

To conduct our operations more smoothly, we may disclose the Personal Data you have provided to us to our third-party services providers, agents and/or affiliates or related corporations (“External Parties”) for such External Parties to process your Personal Data based on your requested services for one or more of the above stated reasons or purposes. An External Party may be sited locally or outside Singapore.

3.5.

If we need to use your Personal Data for any other purposes, we will notify you and obtain your consent beforehand in accordance with the requirements of applicable data protection laws.

4. Accuracy of Personal Data

4.1.

We will take appropriate and reasonable steps to ensure the accuracy and correctness of the Personal Data that we collect, use and/or disclose. To enable us to ensure the quality and accuracy of Personal Data, you have an obligation to provide accurate and up-to-date information to us.

5. How We Protect Your Personal Data

5.1.

We will take reasonable efforts to protect the Personal Data in our possession or under our control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. However, we cannot completely guarantee the security of any Personal Data we may have collected from or about you, e.g. that no harmful code (such as viruses, bugs, Trojan horses, spyware or adware) will enter our website.

6. How Long Do We Retain Your Personal Data

6.1.

We retain Personal Data as may be required for business, legal, regulatory or compliance purposes, and such purposes do vary according to the circumstances. We will take reasonable steps to dispose or anonymise Personal Data that is no longer needed. With regard to medical

data that we process, we will retain medical records in accordance with the duration stipulated by the Ministry of Health or/and in adherence with contractual agreements.

7. Transfer of Personal Data Outside Singapore

7.1.

Generally, we do not transfer Personal Data out of Singapore, except to our approved third party services providers for applicable services. Should we do so, we will ensure there is compliance with the requirements under the PDPA.

8. Third Party Sites

8.1.

This site may contain links to sites whose data protection and privacy practices may differ from ours. We are not responsible for the content and privacy practices of these other websites and encourage you to check the privacy notices of these other websites to determine how they will handle any information they collect from you.

9. Contacting Us – Feedback, Withdrawal of Consent, Access and Correction of your Personal Data

9.1.

You are entitled to withdraw your consent for the collection, use and disclosure of your Personal Data at any time. However, depending on the nature of the withdrawal, it may become impossible for Beacon to provide services such as processing or providing services offered by BPMCCAMP.

9.2.

If you:

(a)

have any questions or feedback relating to your Personal Data or our Privacy Policy;

(b)

would like to withdraw your consent to any use of your Personal Data as set out in this Privacy Policy; or

(c)

would like to obtain access and make corrections to your Personal Data records, you can contact our Data Protection Officer by emailing us at customercare@beacon.com.sg.

10. Governing Law

10.1.

This Privacy Policy shall be governed in all respects by the law of Singapore.