# PRIVACY NOTICE:
# Philips Engage

## This Privacy Notice was last changed on January 28, 2022

Philips offers the Engage web and mobile applications ("App") to healthcare providers to support clinically based patient decision support and to aid in remote communication and care management between patients and healthcare providers. Philips acts as a Data Processor in providing these services on behalf of your healthcare provider (as a Data Controller).

Your healthcare provider is responsible for the processing of your personal data while you utilize the App, including obtaining your consent for your use of the App. In this notice, we will briefly describe what types of personal data are processed per the direction of your healthcare provider.

If you have any questions related to how your healthcare provider requires us to process your data for the purposes of providing you the App, you should inquire with them directly and reference their notice of privacy practices.

### Data Processed on behalf of the Healthcare Provider

When you install and access the App, we will process your personal data as specified below and in general to perform the services requested by and on behalf of your healthcare provider.

### Account Data

When you create a *Philips Engage* account you will need to provide your full name, address, and email address to create account credentials to access the App. When using the App you will be able to view and update your current medical status. You can choose what information you wish to upload into the App. You also have choices related to authorising your healthcare provider to send messages to your account and provide you with care-related information.

The data is used to create and manage your account and to provide the App service.

### Personal and Device Data

Other personal data collected and processed within the App includes: full name, address data, gender, email address, phone number, date of birth, patient unique identifier (e.g. SSN or MRN), marital status, healthcare provider/care team, credentials and health/medical information. This information is collected and needed to provide the services of the App to you.

Device data collected and processed within the App includes: unique user device identifiers, the IP address of your mobile device, session data and usage data.

Health data collected and processed within the App includes: health data stored in Engage, data collected from devices you connected to the app, such as a saturation or blood pressure meter, or data collected from Google Fit / Apple Health.

This data is used by Philips and your healthcare provider to enable the App.

### Cookies

Only functional cookies are used in the App, no other cookies (performance, analytical or marketing) are used.

## Permissions

The App may request your permission to access your phone sensors (e.g. camera, Wi-Fi, geo-location, or Bluetooth) or data (e.g. photos, agenda, or contacts) on your mobile device.

We use such data only when it is needed to provide you the App and only after you provided your explicit consent.

Sometimes the permission is a technical precondition of the operating systems of your mobile device. In such case, the App may ask your permission to access such sensors or data, however we will not collect such data, unless when it is required to provide you the App and only after you provided consent.

Your device location data will only be used to enable Bluetooth services (Android only).

With your explicit consent, the App can import measurements from other mobile apps such as Google Fit and Apple Health and share them with your healthcare provider. You can withdraw your consent at any time to stop such importing and sharing.

## We protect your health data

We recognise and take seriously our responsibility to protect the personal data that you entrust to Philips from loss, misuse or unauthorised access. Philips uses a variety of security technologies and organisational procedures to help protect your personal data. For example, we implement access controls, use firewalls and encryption, and always employ secure servers.