

SMARTZ[®] SYTEM – DATA PRIVACY CONSENT TO USE

- **Who is responsible for collecting and processing your personal information?**
Controller Name: Your Institutional care provider
Processor Name: Smartz Operations Pty Ltd.
Sub-processor Name: Microsoft Azure
- **Definitions**
 - Smartz[®] pod: a wearable device compliant to medical device regulations; the pod is designed to attach to incontinence products to collect sensor data associated with incontinence events, environmental temperature, positioning, and falls
- **What data will be collected for Patient ?**
 - Patient Identifiers: Name
 - Health data: Sensor data associated with a pod and incontinence related data including position and falls.
 - Manual observational data: related to capturing data about the status of used incontinence products, skin health data, care activity and related workflows
- **What data will be collected for Users/non-patient ?**
 - User Information: Email, username, activity logs
 - Application related device data: IP address, operating system
- **How the data will be collected**
 - Encrypted Pod data associated with a patient sent via encrypted networks to a secure cloud database.
 - Manual observational data collected either in direct electronic format or converted from paper formats, an in all cases held in a secure database

SMARTZ® SYTEM – DATA PRIVACY CONSENT TO USE

- **How the data will be used?**

Health data will be processed for the purpose of fulfilling the intended use of the Smartz system including monitoring of voiding events, falls monitoring, ambient temperature, body position and movement.

Collection of health data is to allow users to monitor: voiding events, falls, ambient temperature, body position and movement.

Manual observational data is used to support certain system features, product improvement and for pilot, or trial, evaluation purposes.

User account emails may be used for marketing and communications purpose related to the product. To opt out of these, please contact your data controller

Device attributes may be used for troubleshooting and technical support purposes.

Patient Identifiers are used within the system for grouping and association of Smartz® Pod data.

Location-related information may be used to scan for nearby Bluetooth devices. We do not track information such as current location, where you live or the places you like to go. Our app uses location information solely for the purpose of Bluetooth scanning and discovery of Smartz® Pods.

- **How long will the data be kept?**

The data controller can set the maximum time the personal health data can be stored, based on inactivity. The default maximum time is 12 months since last activity.

- **Storage and Transfer of your information**

Your information is hosted in secure cloud servers in accordance with local privacy regulations. Your information may be transferred across jurisdictional borders in accordance with your regional data privacy regulation.

SMARTZ® SYTEM – DATA PRIVACY CONSENT TO USE

- **Disclosure to third parties**

Controller may disclose your information to the processor such as Smartz Operations Pty Ltd and affiliates where necessary to provide the services to respond to authorized information requests from government or regulatory authorities or when required by law. Information provided to third parties will not be used for their marketing or commercial purposes (unless you have separately and expressly opted in to this) or unless this is required in connection with sale, merger or transfer of a product line.

- **Use of De-identified information**

De-identified, pseudonymised and /or anonymized information may be used

- Smartz service obligations, product development, data analysis or statistical and survey purposes including testing functionality and features, regulatory and improving the Smartz® system.

De-identified and /or anonymized information may be used

- For use by third parties.

- **Rights regarding your information**

Your controller is responsible for managing your personal health data. Through your controller you have :

The right to access – You have the right to request the copies of the personal and health data

The right to rectification- You have the right to request the controller to correct any personal data you believe is inaccurate

The right to erasure – You have the right to request the controller to erase your personal data under certain conditions

The right to data portability- you have the right to request the controller to transfer the data that we collected to another organization

As a data processor Smartz will act on instruction from the data controller. If we receive a request, we have one month to respond. The data controller can contact us at customerservice@smartzhealth.com