Breezing App Privacy Policy

WHAT INFORMATION DOES BREEZING APP COLLECT?

The Breezing App collects metabolic data, which may be stored on iCloud or Google Cloud, or on a user mobile device that has the Breezing Pro™/Breezing MedT™ Mobile Application.

The Breezing App also collects the following personal data, but has no access to the personal data. Only users and/or professional support personnel have access to the personal data:

- First name, last name, sex, date of birth, height, weight, life style, and patient ID

WHY IS DATA COLLECTED?

The metabolic and personal data is collected by users and/or professional support personnel to help develop personalized health management plan for wellness, weight and obesity management.

HOW DOES THE DATA COLLECTED TO BE USED?

Data collected using Breezing Pro™/Breezing MedT™ device is transferred to the App for review by the user and/or professional support personnel. Analyzed data (patient App results) are then synced to the cloud (Cloud Firestore) for data redundancy.

WHAT DATA IS SHARED?

Breezing Co. does not have access to share any patient's test data with any 3rd parties. All data will be used by the users and/or professional support personnel.

HOW THE DATA IS STORED AND PROTECTED

Information Security to protect your information – The
software is designed and will be tested to comply with FDA software guidance documents including:

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 2002
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 11, 2005
- IEC 62304 Medical device software, Software life cycle processes
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rule
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, October 2014 (final) and October 2018 (draft)

Cybersecurity

Breezing's cybersecurity is multifaceted to ensure the security and accuracy of the data provided for Breezing Pro™/Breezing Med™.

Security: Breezing complies with HIPAA, HITECH, and FDA's Cybersecurity guidance (Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, October 2014). Information

Technology, Quality, software development, and management work together to implement policies and procedures across the company designed to ensure security of the device and its data. These systems include physically and electronically restricting access to authorized personnel, monitoring and mitigating vulnerabilities, managing risks, and managing updates and changes to the software. All Breezing data between device and App are encrypted using industry best practices. The transmissions are verified to be correct by a mechanism called checksum, where a small hash is generated from a large set of data in a deterministic way and this is used to confirm that two large sets of data are bit for bit identical. Cyber-threats are detected through the use of numerous technologies.

Cyber-threats: The Breezing infrastructure was examined for possible cyber-threats, and each was assessed using a risk-based-approach for the likelihood of exploitation by assigning each to either a low, medium, or high category. Mitigation measures have been identified, as well as remediation measures that would be taken, in the unlikely event of exploitation.

Discussion of High Likelihood of Exploitation: Two categories have been identified as having a high likelihood of exploitation: data loss/corruption and application code containing bugs. However, neither present a high degree of actual risk to the device due to the design efforts employed to rapidly detect, mitigate, and remedy any such issues. In addition, the ongoing systematic vigilance provides further protection from threats as described in the below sections.

Ongoing Systematic Vigilance and Responsiveness Plan: The following methods comprise the ongoing vigilance for the system, and if any signals are detected, rapid response is implemented. Security Measures for Updates Software or firmware updates are restricted to authenticated code and code signature verification. Code repository is source controlled with specific and limited permissions on an individual basis to prevent manipulation. The code packaging system is immutable and deployment to systems is automated and idempotent. Code verification (unit tests) takes place on infrastructure which is configured identically to the device, code validation (integration/system tests) take place once the code is deployed to the device. Systematic procedures only allow authorized users to download version-identifiable software and firmware from the manufacturers. Manufacturer-provided software, including the device embedded software, is first mirrored internally, added to the software packaging system, and then verified and validated prior to use. Other third-party obtained software is similarly first mirrored internally, evaluated, and verified and validated to prove that the code is functioning and correct prior to implementation. This method is similar to implementation of internally developed tools.

Responsibilities: Defined responsibilities for assuring cybersecurity and software functioning are performed by Breezing's IT group, which is responsible for establishing cybersecurity policy and high-level networking monitoring. Breezing's software development team is responsible for server-level monitoring and endpoint testing.

Potential Impact to Patients: Potential cyber-hazards related to incorrect patient reports include data corruption at rest or in transit, data manipulation at rest or in transit, code manipulation at rest or in transit. Data corruption: low risk for patient harm due to various checksums along the process. Harm would be limited to a delay in receiving results, as data processing would need to restart from the beginning. Data manipulation: moderate risk for patient harm, as results have potential to be altered to add or remove specific findings or recommendations from reports if access to data was obtained and went undetected. However, results are reviewed by the professionals prior to report release and the patient's clinician is responsible for making final treatment decisions with data in the context of the overall treatment plan. Code manipulation: moderate risk for patient harm as results have potential to be

incorrect or incomplete. However, results are reviewed and not directly diagnostic or therapeutic as above described.

DISCLAIMERS

1. SECURITY AND PRIVACY

a. Breezing Pro Co. or its licensors, in their sole discretion, have taken measures to protect the privacy, integrity and security of the data entered by the user when transmitting that data between the user's device(s) such as iPhone, iPad, or a web browser and the servers that may host/store the metabolic data. You acknowledge, however, that: (i) despite these security and privacy measures, it is possible that there can be a breach in the data security resulting from non-malicious actions of Breezing Pro Co. or its licensors and/or malicious actions of external parties; and (ii) neither Breezing Co. nor its licensors will be responsible for such effects.

b. Security Breaches. (a) Each Breezing user shall, promptly after confirmation thereof, notify Breezing Co. of any actual, probable or reasonably suspected breach of any safeguards or of any other actual, probable or reasonably suspected unauthorized access to, or acquisition, use, loss, destruction, compromise or disclosure of, any Subscriber Information maintained on such Information Party's systems (each, a "Security Breach"). In any notification to Breezing Co. required, the Information Party shall designate a single individual employed by such Information Party who shall be reasonably available to Breezing Co. during regular business hours as a contact regarding such Information Party's obligations under this Section.

APPLICABLE LOCAL LAWS

Data privacy laws outside the USA: Breezing users shall comply with all applicable data privacy laws in the countries where they use and store the test data. It is very important to have complete knowledge of the data and privacy protection laws enforced in that countries and regions your customers and end users are in. Non-compliance with these laws can result in hefty fines or even prosecution against the violator.

USA State data privacy laws: The U.S. has hundreds of sectoral data privacy and data security laws among its states. U.S. state attorney general oversee data privacy laws governing the collection, storage, safeguarding, disposal and use of personal data collected from their residents, especially regarding data breach notifications and the security of Social Security numbers. Some apply only to governmental entities; some apply only to private entities, and some apply to both. In addition to sectoral privacy laws, the U.S. is experiencing a massive push toward pushing privacy legislation at the state level. Breezing users shall comply with all applicable data privacy laws in the state where they use and store the test data.

California Privacy Laws
California laws includes Constitutional Right to Privacy, General Privacy Laws and Health Information Privacy. If you are a California resident, you are entitled to receive data use privacy policy.

YOU HEREBY ACKNOWLEDGE THAT YOU HAVE READ THIS BREEZING APP PRIVACY POLICY, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

If you have any questions, please contact us at info@breezing.co or (480) 629-5360.