Biometric Policy

*Assistance For the Disabled: Alternative formats of this form are available to individuals with a disability. Please contact **(888) 221-7317** for assistance.*

I. APPLICABILITY

This policy applies to all associates of Brookdale Senior Living Inc. ("Brookdale" or the "Company") who, in the course of performing their regular job responsibilities, are involved in the collection, use, handling, safeguarding, storage, retention, and destruction of Biometric Data.

II. PURPOSE AND ROLE

Brookdale recognizes the sensitive nature of Biometric Data and is committed to protecting Biometric Data. In an effort to further this commitment, this Biometric Policy ("Policy") establishes guidance for the collection, retention, and treatment of Biometric Data obtained or received by the Company and/or its vendors.

III. DEFINITIONS

For purposes of this policy, the following definition shall apply:

A. "Biometric Data" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual.

1. "Biometric Data" can include fingerprints, voiceprints, a retina scan, and scans of hand or face geometry.

2. "Biometric Data" does not include: 1) information captured from a patient in a health care setting or information collected used, stored for health care treatment, payment or operations under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA); 2) a digital or physical photograph, video, or voice recording in themselves, but would include data generated by the technological processing, measurement, or analysis of this content that could be, or is used, for identification purposes.

IV. POLICY

A. **Collection of Biometric Data by the Company:** As required by applicable law, Brookdale will provide notice and obtain consent prior to collecting Biometric Data. Such notice may include a description of the purpose for which the Company intends to use the Biometric Data, how long the Biometric Data will be retained, disclosures of Biometric Data to processors, and the purpose of disclosures to processors. To the extent required by law, Brookdale will obtain fresh consent for processing new categories of Biometric Data or processing Biometric Data for a secondary use.

B. **Prohibited Conduct:** The Company will not sell, lease, trade, or otherwise profit from a person's Biometric Data. Brookdale will not access Biometric Data collected by an associate's or independent contractor's company-issued device.

C. **Restrictions on Brookdale's Disclosure of Biometric Data:** In accordance with applicable law, Brookdale will not disclose Biometric Data unless and until (a) the individual provides written consent for the disclosure; (b) the Company is compelled to disclose the Biometric Data pursuant to a valid warrant or subpoena; or (c) the Company is required to disclose the information by law.

D. **Security for Biometric Data Collected by Brookdale:** The Company will implement administrative, technical, and physical safeguards for Biometric Data that are at least as stringent as the safeguards which has implemented for its other confidential information. In addition, Biometric Data in electronic form will be encrypted when in storage. Paper documents containing Biometric Data, when unattended, will be stored in a locked filing cabinet, storage area, or office. Only associates with a legitimate business need may access Biometric Data. Authorized associates should avoid creating paper documents containing Biometric Data whenever possible. No associate may disclose Biometric Data to any third party without the prior authorization of the Legal Department.

E. **Biometric Security Incident Response:** Any associate who becomes aware of the unauthorized access or acquisition of Biometric Data ("Biometric Security Incident") must immediately contact **the Company's Privacy Officer at privacyofficer@brookdale.com or via telephone at (414) 918-5211**. As soon as reasonably possible, Brookdale will (a) investigate any report of a Biometric Security Incident, (b) stop the Biometric Security Incident, (c) determine whether the Biometric Security Incident is a data breach under applicable law, and (d) implement steps to prevent a recurrence of the Biometric Security Incident. If Brookdale determines that a breach of Biometric Data has occurred, Brookdale will provide breach notifications and services in accordance with applicable law.

F. **Retention of Biometric Data:** Unless otherwise required by law, Brookdale will permanently destroy an individual's Biometric Data from Brookdale's systems, or the systems of Brookdale's vendor(s), on or before the earliest of the following dates:

1. When the initial purpose of collection is satisfied;

2. Within 24 months after Brookdale's last interaction with the individual; or

3. Within forty-five days of when storage of the Biometric Data is no longer necessary, adequate, or relevant to the express processing purpose identified by a review conducted by Brookdale at least once annually.

G. **Destruction of Biometric Data:** Paper documents containing Biometric Data will be shredded or burned. Biometric Data in electronic form will be destroyed in a manner that renders the information irretrievable. Brookdale's Human Resources and Information Technology departments shall be responsible for directing the destruction of such information upon expiration of the retention period described in paragraph F, above.

V. CONSEQUENCES OF NON-COMPLIANCE

Violations of this policy or its procedures will result in disciplinary actions under the Company's discipline policy, and may include suspension or termination of employment in the case of severe or repeat violations.

ATTACHMENT A

NOTICE CONCERNING THE PROCESSING OF BIOMETRIC DATA

Brookdale Senior Living Inc. (the "Company") hereby provides notice to the individual named below that:

1. The Company uses a time management system (TMS), supported by Brookdale's vendor Kronos, to manage timekeeping for all hourly, non-exempt associates.

2. To use the TMS, associates will need to provide a scan of their fingertip. The fingertip image is converted to an encrypted algorithm, which cannot be used to recreate the actual fingerprint, and the algorithm is stored in the TMS ("TMS Biometric Data"). The Kronos system does not store the actual fingertip image, just the encrypted algorithm. The TMS then uses the algorithm to verify the fingertip of the individual each time they clock-in or clock-out from work.

3. Brookdale only uses the TMS Biometric Data to verify the identity of the individual clocking in/out from work. The Company uses the attendance records from TMS to manage payroll and attendance, comply with legal obligations, and to ensure compliance with Company policies.

4. The individual may elect to use a finger or facial scan to authenticate their identity on company-issued devices ("Device Biometric Data") rather than using a passcode. The Device Biometric Data is stored on the device and is not accessed by the Company.

5. You may revoke your consent to the collection of any Biometric Data by contacting **the Company's Privacy Officer at privacyofficer@brookdale.com or via telephone at (414) 918-5211**. However, please note that using the TMS is a condition of employment.

6. Except when required by law to retain Biometric Data for a longer period, the Company will not retain Biometric Data for more than 45 days after the associate's employment relationship with, or the contractor's engagement by, the Company has terminated.

7. Within 45 days of the termination of the employment or contractor relationship, the Company will permanently destroy the individual's Biometric Data.