Biometric Data Security Policy

I. APPLICABILITY

This policy applies to all associates of Brookdale Senior Living Inc. (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 Identifiers and Biometric Information (collectively, "Biometric Data").

II. PURPOSE AND ROLE

The Company recognizes the need to maintain the confidentiality of Biometric Data and understands that such data is unique to each individual. The data covered by this Policy may come from various types of individuals performing tasks on behalf of the Company, including associates and independent contractors. The scope of this Policy is intended to be comprehensive and will include Company requirements for the security, storage, and protection of Biometric Data throughout the Company and its approved vendors both on and off work premises.

III. DEFINITIONS

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

A. **"Biometric Identifier"** includes a fingerprint, iris or retina scan, or a scan of hand or face geometry. Biometric identifiers do not include:

1. Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.
2. Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).
3. An X-ray, MRI, PET scan, mammogram, or other image or film of the human anatomy used to diagnose or treat an illness or other medical condition or to further validate scientific testing or screening.

B. **"Biometric Information"** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

C. **"Biometric Data"** refers collectively to all Biometric Identifiers and Biometric Information.

IV. POLICY

A. **Collection of Biometric Data by the Company:** Before collecting Biometric Data from an associate or independent contractor, the Company will provide the individual with a copy of the notice attached to this Policy as Attachment A. The notice explains the specific purpose of the collection of Biometric Data, and obtains the individual's written consent to the collection.

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

C. **Restrictions on the Company's Disclosure of Biometric Data:** The Company will not disclose or otherwise disseminate Biometric Data unless:

1. The subject of the Biometric Data consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
2. The disclosure completes a financial transaction requested or authorized by the subject of the Biometric Data;
3. The disclosure is required by state or federal law; or
4. The disclosure is made to a law enforcement agency for a law enforcement purpose in response to a warrant.

D. **Security for Biometric Data Collected by the Company:** The Company will implement administrative, technical, and physical safeguards for Biometric Data that are at least as stringent as the safeguards which the Company 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. **Retention of Biometric Data:** All Biometric Data will be destroyed within 90 days of the:

1. The employment termination date, in the case of an associate;
2. The contract termination date, in the case of an independent contractor.

To the extent permitted by applicable law or required by court order, the Company will suspend the destruction of Biometric Data when, and to the limited extent, necessary to satisfy the Company's duty to preserve information that would be discoverable in litigation.

F. **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. The Company'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 E, 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 INFORMATION

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

1. The Company utilizes biometric information in its payroll timekeeping processes, as applicable, to authenticate the individual's identity ("Payroll Biometric Information"). Payroll Biometric Information, for purposes of this Notice, consists of a data set based on the distance between points on an image of the individual's fingerprint. The timekeeping process **does not** store an image of the fingerprint itself.

2. The individual may elect to use biometric information to authenticate their identity on company-issued devices ("Device Biometric Information") rather than using a passcode. The Device Biometric Information is stored on the device and is not accessed by the Company.

3. Except when required by law to retain the biometric information for a longer period, the Company will not retain this biometric information for more than 90 days after the associate's employment relationship with, or the contractor's engagement by, the Company has terminated.

4. Within 90 days of the termination of the employment or contractor relationship, the Company will permanently destroy your biometric information.

AUTHORIZATION CONCERNING BIOMETRIC INFORMATION

I have reviewed, and I understand, the Notice Concerning Processing of Biometric Information, above. I hereby consent to Brookdale Senior Living Inc.'s collection, use, and retention of my biometric information as described above.

Printed Name: _____

Signature: _____

Date: _____