BIOMETRIC INFORMATION PRIVACY POLICY

Asbury LLC ("the Company") intends to cooperate with the Illinois Biometric Information Act, 740 ILCS ("BIPA") 740 ILCS §14/1, *et seq.* ("BIPA"). The Company, therefore, has instituted the following biometric information privacy policy with regards to biometric information collected from residents and visitors (together, "Individuals") and Employees.

DEFINITIONS

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in BIPA.

Biometric identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include the following: writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, physical descriptions such as height, weight, hair color, or eye color, or 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.

Biometric information means any information, regardless of how it is captured, converted, stored, or shared, based on a person'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.

PURPOSES FOR COLLECTION OF BIOMETRIC DATA

The Company uses facial technology ("the Facial Scan Device") and finger scan technology ("the Finger Scan Device," together, "the Devices") for Individual and Employee temperature screening and Employee timekeeping purposes, respectively.

- The Facial Scan Device uses a scanner that measures temperature of Individuals and Employees and collects representations of the scan of their faces. The biometric feature of the Facial Scan Device collects the data generated by the facial scan to authenticate a person's identity and, through synchronization with the facility's access controls, allow him or her to enter the building.
- The Finger Scan Device uses a scanner that collects an encrypted representation of a scan of an Employee's finger. The biometric feature of the Finger Scan Device uses data collected from a scan of an Employee's finger to allow him or her to clock in and out of the Company's timekeeping system. If an Employee decides to enroll in this feature of the Device, a biometric scanner will capture and collect data from his or her finger to create a unique template that is a mathematical representation of the finger to authenticate the Employee's identity for timekeeping purposes.

DISCLOSURE AND AUTHORIZATION

Written permission to collect biometric identifiers and/or biometric information must be provided by the Individual or Employee prior to collection of such data. The Company will not collect,

capture, purchase, receive through trade, or otherwise obtain biometric information related to the employee without first:

1. Informing the Individual, Employee, or their legally authorized representative in writing that it is being collected or stored;
2. Informing the Individual, Employee, or their legally authorized representative the specific purpose and length of term for which biometric data of the employee is being collected, stored, and used; and
3. Receiving a written release executed by the Individual, Employee, or their legally designated representative to collect, store, and use the employee's biometric information for the specific purposes the Company disclosed.

Once collected, the Company will not sell, lease, or trade any biometric identifiers or biometric information collected.

DISCLOSURE OF DATA

The Company will not disclose or disseminate any biometric identifiers and/or biometric information without/unless:

1. First obtaining the Individual's or Employee's (or their legally authorized representative's) written consent to such disclosure or dissemination;
2. The disclosed information completes a financial transaction authorized by the Individual or Employee or their legally authorized representative;
3. Disclosure is required by state or federal law; or
4. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

RETENTION & DESTRUCTION OF DATA

Employee biometric data and/or biometric information will be collected, stored, used, and retained only as long as you are employed with the Company and will be destroyed within thirty (30) days of your separation of employment unless the Company is required by law to retain the data for longer.

Individuals' biometric data and/or biometric information will be destroyed when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the Individual's last interaction with the Company, whichever occurs first, unless the Company is required by law to retain the data for longer.

SECURITY OF DATA

The Company will use a reasonable standard of care to store, transmit, and protect from disclosure or dissemination any paper or electronic biometric data collected. Reasonable standard of care is defined as using similar or better means of storing other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.