

## PURPOSE

The purpose of this policy is to define the policy and procedures for the collection, use, safeguarding, storage, retention, and destruction of biometric data in compliance with all laws, including, but not limited to, the Illinois Biometric Information Privacy Act, 740 ILCS Section 14/1, *et seq.*

## POLICY STATEMENT

Lifespace Communities, Inc., its affiliates and subsidiaries (“Lifespace”) policy is to protect, use and store biometric data in accordance with all applicable laws including, but not limited to, the Illinois Biometric Information Privacy Act. This policy outlines the procedures for the collection, use, safeguarding, storage, retention, and destruction of biometric data gathered by or associated with the system(s) utilized by Lifespace for team member timekeeping.

## DEFINITIONS

**Biometric Identifiers:** A retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions. Biometric identifiers do not include 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”).

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

**Biometric Data:** Includes both Biometric Identifiers and Biometric Information.

## PROCEDURES

Working with the time and attendance system vendor, Lifespace uses intelligent terminals which utilize biometric data for the purpose of team member timekeeping. The time and attendance system vendor provides the terminals and collects and stores the biometric data at issue (specifically, fingerprint scans). Lifespace uses these intelligent terminals to document team members’ time clock activities, such as clocking in and out of shifts and/or clocking in and out for meal breaks. The length of term for biometric retention is for the duration of a team member’s employment.

Lifespace does not have access to the biometric data stored in the intelligent terminals and on system servers. Lifespace will not sell lease, trade, or otherwise profit from a team member's biometric data. Lifespace will not request the vendor to disclose biometric data unless a) consent is obtained, b) disclosure is required by law, or c) disclosure is required by a valid subpoena.

It is Lifespace's policy to destroy any team member biometric data in the system upon the effective date of a team member's resignation, retirement, or termination from Lifespace; or within a reasonable amount of time.

The timekeeping vendor has represented that they protect the biometric data gathered in compliance with applicable laws. The vendor has further represented that it will take reasonable steps to store, transmit, and protect from disclosure any biometric data of Lifespace team members in its possession, and will protect the data in the same or in a more protective manner than it stores and transmits its own confidential and sensitive information. The vendor has further represented that it will not disclose any Lifespace team member biometric data to any third party unless a) consent is obtained, b) the disclosure is necessary to the completion of a financial transaction requested or authorized by the individual, c) the disclosure is required by law, or d) the disclosure is required by valid subpoena.

The communities' human resources departments will obtain the consent of all team members employed in Illinois who will utilize the timekeeping intelligent terminals and/or the timekeeping system prior to the collection of biometric data. In the event that Lifespace or the vendor's handling of team member biometric data changes in the future, this policy will be updated.

## **RELATED DOCUMENTATION AND REFERENCES**

4-208.1 *Biometric Information Privacy Team Member Consent Form*

## **REVIEW FREQUENCY**

Every three years or on or before the effective dates of applicable rules and regulations.