BIOMETRIC INFORMATION PRIVACY POLICY

Biometric Data Defined

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. "Biometric identifier" means 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 valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. 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.

"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.

Purpose for Collection of Biometric Data

Alivio Medical Center ("Alivio"), its vendors, and/or the licensor of Alivio's time and attendance software collect, store, and use biometric data solely for employee identification, fraud prevention, and pre-employment hiring purposes.

Alivio, its vendors, and/or the licensor of Alivio Medical Center's time and attendance software will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that Alivio's vendors and the licensor of Alivio 's time and attendance software may be paid for products or services used by Alivio that utilize such biometric data.

Disclosure
Alivio will not disclose or disseminate any biometric data to anyone other than its vendors and the licensor of Alivio's time and attendance software providing products and services using biometric data without/unless:

- First obtaining written employee consent to such disclosure or dissemination;
- The disclosed data completes a financial transaction requested or authorized by the employee;
- Disclosure is required by state or federal law or municipal ordinance; or
- Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

Alivio shall retain employee biometric data only until, and shall request that its vendors and the licensor of Alivio's time and attendance software permanently destroy such data when, the **first** of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with Alivio, or the employee moves to a role within Alivio for which the biometric data is not used; or
- Within 3 years of the employee's last interaction with Alivio.

Data Storage

Alivio shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which Alivio stores, transmits and protects from disclosure 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.

BIOMETRIC INFORMATION PRIVACY
EMPLOYEE CONSENT FORM

The employee named below has been advised and understands that Alivio Medical Center, its vendors, and/or the licensor of Alivio Medical Center's time and attendance software collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing Alivio Medical Center's biometric timeclocks or timeclock attachments. Biometric timeclocks are computer-based systems that scan an employee's finger for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the employee's identity, for example, when the employee arrives at or departs from the workplace.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), regulates the collection, storage, use, and retention of "biometric identifiers" and "biometric information." "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "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.

The employee understands that he or she is free to decline to provide biometric identifiers and biometric information to Alivio Medical Center, its vendors, and/or the licensor of Alivio Medical Center's time and attendance software without any adverse employment action. The employee may revoke this consent at any time by notifying Alivio Medical Center in writing.

The undersigned employee acknowledges that he/she has received the attached *Biometric Information Privacy Policy*, and that he/she voluntarily consents to Alivio Medical Center's, its vendors', and/or the licensor of Alivio Medical Center's time and attendance software's collection, storage, and use of biometric data through a biometric timeclock, including to the extent that it utilizes the employee's biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to Alivio Medical Center providing such biometric data to its vendors, and/or the licensor of Alivio Medical Center's time and attendance software.

_____
Employee Signature   Date

_____
Employee Name (print)

216780751.1 09999/09998-3081