BIOMETRIC INFORMATION PRIVACY POLICY AND CONSENT

Advanced Medical Transport of Central Illinois ("The Company") has instituted the following Biometric Information Privacy Policy ("Policy"):

Purpose

The Policy defines the Company's policy and procedures for collection, use, safeguarding, storage, retention, and destruction of biometric data collected by the Company and/or its vendors in accordance with the applicable laws including, but not limited to, the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, *et seq*.

Given the public health concerns related to the COVID-19 pandemic, the Company will use an infrared sensor device to screen temperatures of employees. The device will identify the employees of the Company using facial recognition technology and measure forehead temperatures. The device will also detect if employees are wearing face masks. At a minimum, these devices will be installed at all entrances in Peoria and outer markets of the Company. The purpose of the device is to enable the Company to monitor its employees for fevers and mitigate the spread of COVID-19 in the workplace. The Company and/or its vendors collect, store, and use employee biometric data for the purpose of monitoring employees for fevers and ensuring that they are wearing face masks.

An employee's biometric data will not be collected or otherwise obtained by the Company without prior written consent and release by the employee. The Company will inform the employee of the reason his or her biometric information is being collected and the length of time the data will be stored.

Definition

Biometric data means personal information stored by the Company and/or its vendors about an individual's physical characteristics that can be used to identify that person. As used in this Policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois BIPA, 740 ILCS § 14/10.

"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 biological materials regulated under the Genetic Information Privacy Act. 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 the 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.

Disclosure

To the extent that the Company and/or its vendors collect, capture, or otherwise obtain biometric data relating to an employee, the Company will first:

a. Inform the employee in writing that the Company and/or its vendors are collecting, capturing, or otherwise obtaining the employee's biometric data, and that the Company is providing such biometric data to its vendors;
b. Inform the employee in writing of the specific purpose and length of time for which his or her biometric data is being collected, stored, and used; and
c. Receive a written release signed by the employee (or his or her legally authorized representative) authorizing the Company and/or its vendors to collect, store, and use the employee's biometric data for the specific purposes disclosed by the Company, and for the Company to provide such biometric data to its vendors.

The Company and/or its vendors will not sell, lease, trade, or otherwise profit from an employee's biometric data; provided, however, that the Company's vendors may be paid for products or services used by the Company that utilize such biometric data.

The Company will not disclose or disseminate any biometric data to anyone other than its vendors without/unless:

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

Retention schedule

The Company shall retain employee biometric data only until, and shall request that its vendors permanently destroy such data when, the first of the following occurs:

a. The initial purpose for collecting or obtaining such biometric data has been satisfied; or
b. Within three (3) years of the employee's last interaction with the Company.

Data Storage

The Company 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 the Company 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.

Consent Form

Each employee as a condition of employment and/or continued employment must execute a copy of the Consent Form attached to this Policy.