CARLINVILLE AREA HOSPITAL

ADMINISTRATIVE POLICY

No. 093

SUBJECT: Biometric Information Privacy

The Carlinville Area Hospital Association (the "Hospital") has adopted this Biometric Information Privacy Policy in accordance with the Illinois Biometric Information Privacy Act, 740 ILCS §§ 14/1 – 14/99 ("BIPA"). This policy is to be construed and administered in compliance with BIPA and any other applicable federal or state laws and shall be made publicly available at https://www.cahcare.com/.

Definitions

"Biometric Data" means any "Biometric Identifier" or "Biometric Information."

"Biometric Identifier," as defined in BIPA, 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 Identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric Information," as defined in BIPA, 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 Identifier.

Purpose of Collection

The Hospital, its vendors, and/or the licensors of the hospital's products and services may collect, store, and use employee Biometric Data solely for the purpose of giving employees secure access to drug cabinets or other pharmacy-related equipment or machines. In addition, facial geometry is used for facial recognition for purposes of timekeeping with the Hospital's time clocks. If the Hospital begins collecting Biometric Data for any additional purpose, the Hospital will update this procedure.

Collection

Prior to collecting, capturing, or otherwise obtaining Biometric Data relating to an employee, the Hospital will first:

a. Inform the employee in writing that his or her Biometric Data or one or more Biometric Identifiers is/are being collected, stored, and used;

b. Inform the employee in writing of the specific purpose and length of term for which the Biometric Data/Biometric Identifier(s) is/are being collected, stored, and used; and

c. Obtain a written release executed by the employee or his or her legally authorized representative.

A sample release is attached to this policy. The employee may decline to provide or revoke his or her release in writing at any time. However, the employee's execution of a release is a condition of his or her employment with the Hospital in order to access drug cabinets or pharmacy- related equipment and/or to record the employee's time worked each work day. Any failure to provide an executed release or the revocation of a release may preclude any employment with the Hospital, result in the termination of the employee's employment with the Hospital, result in a transfer of the employee to a role within the Hospital for which such Biometric Data are not used, and/or result in other material changes in the employee's employment with the Hospital, as determined by the Hospital in its sole discretion.

Storage

The Hospital will 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 Hospital 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.

Prohibited Uses

The Hospital will not sell, lease, trade, or otherwise profit from employees' Biometric Data; provided, however, that the Hospital's vendors and licensors may be paid for products or services used by the Hospital that utilize such Biometric Data.

Permitted Redisclosures

The Hospital will not disclose or disseminate any Biometric Data to anyone other than its vendors and the licensors of the Hospital's products and services that use such Biometric Data, unless:

a. The employee or his or her legally authorized representative consents to the disclosure or redisclosure;

b. The disclosure or redisclosure completes a financial transaction requested or authorized by the employee or his or her legally authorized representative;

c. The disclosure or redisclosure is required by state or federal law or municipal ordinance; or

d. The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

Unless a valid warrant or subpoena issued by a court of competent jurisdiction provides otherwise, an employee's Biometric Data shall be destroyed on the earliest of the following to occur:

a. When the initial purpose for collecting or obtaining such Biometric Data has been satisfied, such as the termination of the employee's employment with the Hospital, or the transfer of the employee to a role within the Hospital for which Biometric Data are not used; or

b. Within three (3) years of the employee's last interaction with the Hospital.

President/CEO

02/07/2023
Date

Revised 02/2023

RELEASE

I, the employee named below, have been advised and understand that Carlinville Area Hospital Association (the "Hospital"), its vendors, and/or the licensors of the Hospital's products and services will collect, store, and use my fingerprints, a fingerprint template based on my fingerprints, facial geometry/facial recognition factors or other Biometric Data (as defined in the Hospital's Biometric Information Privacy Policy) for the purpose of verifying my identity in order to provide me access to drug cabinets or other pharmacy-related equipment or machines, and/or to record my time worked in the Hospital's timekeeping system. I voluntarily consent to the collection, storage, and use of my Biometric Data by the Hospital, its vendors, and/or the licensors of the Hospital's products and services in accordance with the Hospital's Biometric Information Privacy Policy for such purposes.

My Biometric Data will not be sold and may only be redisclosed in limited circumstances, as explained in the Hospital's Biometric Information Privacy Policy. Unless a valid warrant or subpoena issued by a court of competent jurisdiction provides otherwise, my Biometric Data will be destroyed on the earliest of the following to occur: (1) when the initial purpose for collecting, storing, or using my Biometric Data has been satisfied, such as the termination of my employment with the Hospital, or my transfer to a role within the Hospital for which Biometric Data are not used; or (2) within three (3) years of my last interaction with the Hospital.

I further understand that my consent to provide my Biometric Data to the Hospital, its vendors, and/or the licensors of the Hospital's products and services is required for my position for purposes of my having secure access to drug cabinets and/or pharmacy-related equipment and/or machines and/or for purposes of recording my working time. Should I desire to revoke this consent at a future date, revocation must be in writing. I understand that, should I decide to revoke my consent in the future, this may result in a situation where I am no longer permitted to continue employment in my current position. Exclusion from this requirement would be permitted only for those with a physical condition that would make the capture of fingerprint biometric data and/or facial geometry/facial recognition impossible.

I further acknowledge that I have read and understand the Hospital's Biometric Information Privacy Policy, which is accessible online at https://www.cahcare.com/.

_____

Employee's Signature

_____

Employee's Name (Print)

_____

Date