Well Child Center Biometric Information Privacy Policy

Well Child Conference of Elgin d/b/a Well Child Center, and its affiliates, partners, our third-party timekeeping vendor, and/or our third-party timekeeping licensor (collectively "WCC", "we", "us" and "our"), is a not-for-profit organization providing dental care and nutrition education, counseling and support for children and families.

This Biometric Information Privacy Policy ("Biometric Policy") explains how WCC collects, stores, and uses biometric information provided to us by you or our third-party timekeeping vendor and/or our third-party timekeeping licensor, which identifies or could be used to identify you, as further described, below.

This Biometric Policy is publicly available on the WCC website (www.wellchildcenter.org).

Definition

As used in this Biometric Policy, the term "biometric identifiers" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry as defined in the Illinois Biometric Information Privacy Act, 740 ILCS 14/10. The term "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 as defined by the Illinois Biometric Information Privacy Act, 740 ILCS 14/10. The term "biometric information" does not include information derived from items or procedures excluded under the definition of biometric identifiers as set forth in the Illinois Biometric Information Privacy Act, 740 ILCS 14/10.

Purpose and Scope

This Biometric Policy explains WCC policy and procedures for collection, use, safeguarding, storage, retention and destruction of biometric data collected by WCC, our third-party timekeeping vendor, and/or our third-party timekeeping licensor in accordance with the applicable laws in the places where we or our clients operate including, but not limited to, the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*.

WCC may utilize timeclocks with biometric scanning features (which may include, but is not limited to, scanning your fingerprint, handprint, retina, iris, or face) to identify you and ensure that you are paid for all hours worked.

WCC will not collect or otherwise obtain your biometric information without your prior written consent and release. This Biometric Policy informs you of the reason your biometric information may be collected and the length of time the information will be stored.

WCC is not responsible for and has no control over the privacy and data security of our third-party timekeeping vendor and/or our third-party timekeeping licensor, which may differ from those explained in our Biometric Privacy Policy.

Collection, Use, Storage and Retention

WCC, our third-party timekeeping vendor and/or our third-party timekeeping licensor may collect, store, and use employee biometric information (such as a retina or iris scan, fingerprint, or scan of hand or face geometry) for the purpose of recording and monitoring employee's hours worked. WCC only uses biometric information for identity verification, workplace security, and fraud prevention purposes.

If you use the biometric scanning feature on one of our timeclocks, we may store that biometric information at a site controlled by WCC or one of our third-party vendors or third-party licensors, or in a cloud environment controlled by WCC or one of our third-party vendors or third-party licensors. WCC and our third-party timekeeping vendor as well as our third-party timekeeping licensor use reasonable standard of care to store, transmit, and protect from disclosure any electronic biometric information collected that is the same as or more protective than the manner WCC uses to protect its own information.

WCC does not sell, lease, trade, or otherwise profit from an individual's biometric identifiers and/or biometric information. WCC will not disclose, redisclose or otherwise disseminate an individual's biometric identifier or biometric information unless: (1) the individual consents in writing to the disclosure; (2) the disclosure or redisclosure is necessary to complete a financial transaction request or authorized by the individual; (3) the disclosure or redisclosure is required by law; or (4) the disclosure or redisclosure is required by a warrant or subpoena.

WCC only stores an individual's biometric identifiers and/or biometric information for so long as a person continues to be actively employed by WCC. Biometric information is deleted no later than last paycheck received by separated employee. In no case is an individual's biometric identifiers and/or biometric information stored for more than three years after that person has stopped being actively employed by WCC.