TimeIPS Timekeeping Biometric Information Privacy Policy

Privacy Policy

To the extent that TimeIPS may come into possession of biometric identifiers or biometric information for anyone covered by the BIPA or similar privacy laws, this written policy, made available to the public, covers the TimeIPS privacy policy for such biometric data.

Definitions (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 donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. 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 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" 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.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.
(Source: P.A. 95-994, eff. 10-3-08.)

TimeIPS Biometric Data Processing

Some electronic timeclocks manufactured by TimeIPS, when equipped with a biometric device such as a fingerprint or hand scanner, may collect, process and store Biometric Data for the purpose of improving the accuracy of recorded time events.

TimeIPS timeclocks are computerized terminals used to collect time and attendance data for employees. When equipped with a biometric device, a scan of a fingerprint or hand can create a “template” using an algorithm specific to, and internal to, the biometric device itself. The template is not a fingerprint or hand scan, nor even a representation of one. The template is a complex number or “hash” that can be used by the same biometric device to judge, in the future, a presented fingerprint or hand to assess the similarity to the one presented originally. The data stored by TimeIPS timeclocks is used to improve accuracy, but is not able to uniquely identify an individual. Specifically, employees must first identify themselves at the timeclock by providing a badge or badge number. Only then will the timeclock request biometrics and assess the chance that presented finger or hand matches the one originally provided by the already identified employee.

Biometric templates are collected, stored and processed solely to help verify the identity of an employee using the time and attendance system, and are not used for any other purpose.

Retention Schedule

TimeIPS has a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 1 year of the individual's last interaction with TimeIPS or a TimeIPS timeclock, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, TimeIPS, if in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines. TimeIPS will only retain employee Biometric Data only until the date the first of the following occurs:

a) the initial purpose for collecting or obtaining such Biometric Data has been satisfied, specifically the employee clocking in or out at a timeclock, or
b) termination of the employee’s employment, or
c) a change to the employee’s employment such that Biometric Data is no longer used, or
d) one year has passed since the Biometric Data was used, or
e) one year has past since the individual’s last interaction with TimeIPS or a TimeIPS timeclock

Biometric data are permanently destroyed by TimeIPS systems automatically based on the criteria above with daily clean-up processes. In addition, information related to biometric data will be removed by TimeIPS systems automatically within 1 year of creation.

Disclosure, Data Storage, Company Usage, Transmission, and Protection

TimeIPS will not sell, lease, trade, or otherwise profit biometric identifiers or biometric information. TimeIPS shall:

(a) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
(b) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

TimeIPS will not disclose, redisclose, or otherwise disseminate biometric identifiers or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Employee Release and Consent

Before using the biometric option on any TimeIPS timeclock, the owner of the timeclock, normally the employee’s employer, must ask the employees to provide informed written consent authorizing TimeIPS and their employer to collect, process and store biometric information and/or biometric identifiers for the purpose of improving time and attendance data accuracy. Employees must have the option to decline this consent and use the time and attendance system without biometric validation. Specifically, in compliance with the following:

a) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
    1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
    2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
    3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

TimeIPS Customer and/or Employer Responsibility

Any customer of TimeIPS or employer using the TimeIPS timeclock biometric capability must comply with all laws related to biometric privacy. For example, but not limited to the following:

a) Review and comply with all applicable laws governing the collection, use, storage, transmission and processing of biometric data conducted or facilitated.
b) To the extent required by law, develop and adopt a Biometric Information Privacy Policy.
c) Provide Biometric Information Privacy Policy to employees and TimeIPS.
d) To the extent required by law, obtain a written release and consent to collect, process, use, transmit and store biometric data from employees for both the Employer and TimeIPS, prior to collecting or using any biometrics.
e) Provide copies of all employee written release and consent forms to TimeIPS.
f) If/when employees revoke consent to collect, process and store biometric data, immediately disable biometrics for the employee in any TimeIPS system used by the employer and notify TimeIPS.
g) Keep TimeIPS software and timeclocks updated to ensure handling and retention of biometric data is done in compliance with the current version of this Biometric Information Privacy Policy.