

## **BIOMETRIC INFORMATION PRIVACY POLICY**

The purpose of this policy is to define the policy and procedures for the collection, use, safeguarding, storage, retention, and destruction of biometric data. It is Provider Plus, Inc.'s policy to protect, use and store biometric data in accordance with the applicable laws including, but not limited to, the Illinois Biometric Information Privacy Act.

Provider Plus, Inc. ("The Company") has instituted the following 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.

### **The Company's Collection of Biometric Data**

The Company, its vendors, and/or the licensor of the Company's time and attendance software collect, store, and use biometric data for the purpose of identifying employees and recording time entries when utilizing the Company's biometric timeclocks or timeclock attachments.

Biometric timeclocks are computer-based systems that scan an employee's finger or hand 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.

This data is collected, stored, and used solely for employee identification, fraud prevention, and pre-employment hiring purposes.

### **Disclosure**

To the extent that the Company, its vendors, and/or the licensor of the Company's time and attendance software collect, capture, or otherwise obtain biometric data relating to an employee, the Company:

- a. Will inform the employee about the collection, storage, and use of such biometric data

- b. Will inform the employee of the specific purpose and length of time for which the biometric data is being collected, stored, and used
- c. Will receive a written release signed by the employee (or his or her legally authorized representative) authorizing The Company, its vendors, and/or the licensor of the Company's time and attendance software 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 and the licensor of The Company's time and attendance software.
- d. Will not disclose, redisclose, or otherwise disseminate an employee's biometric data unless:
  - 1. the employee or the employee's legally authorized representative consents to such disclosure or redisclosure;
  - 2. the disclosure or redisclosure completes a financial transaction requested or authorized by the employee or the employee'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.

### **Retention Schedule**

The Company will retain employee biometric data only until, and will request that its vendors and the licensor of The Company's time and attendance software 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, such as the termination of the employee's employment with The Company, or the employee moves to a role within The Company for which the biometric data is not used; **or**
- b. Within 3 years of the employee's last interaction with The Company.

### **Data Storage, Transmission, and Protection**

The Company will store, transmit, and protect biometric data using a reasonable standard of care. Such storage, transmission, and protection from disclosure will 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 of The Company and its employees.

## BIOMETRIC INFORMATION PRIVACY RELEASE FORM

The employee named below has been advised and understands that Provider Plus, Inc. (“the Company”), its vendors, and/or the licensor of the Company’s time and attendance software collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing the Company’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 the Company, its vendors, and/or the licensor of the Company’s time and attendance software, but that agreeing to provide such biometric identifiers and information is a condition of employment. The employee may revoke this consent at any time by notifying the Company in writing. However, the undersigned employee further acknowledges that consent to the Company’s collection, storage, use, and retention of biometric data is a condition of employment, as authorized by BIPA, 740 ILCS 14/10. Individuals are free to decline or revoke this consent, but doing so will preclude employment by the Company.

The undersigned employee acknowledges that he/she has received the attached Biometric Information Privacy Policy, and that he/she voluntarily consents to the Company’s, its vendors’, and/or the licensor of the Company’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 the Company providing such biometric data to its vendors, and/or the licensor of the Company’s time and attendance software.

---

Signature of Employee or Employee’s legally authorized representative

Date

---

Employee Name (print)