Employer Toolkit

Biometric Time Clocks - What you need to know

Always Designing for People™

Table of Contents

Overview

What are "Biometrics" and Why Should Employers Care?

Author Arthur C. Clarke once said: "Any sufficiently advanced technology is equivalent to magic." Today, technology that once seemed possible only in the realm of science fiction has become routine and even indispensable. The field of biometric authentication, or "biometrics," is an apt example.

The term "biometrics" generally refers to the measurement and analysis of certain biological characteristics of an individual, such as fingerprints, facial geometry, retinal scans, and so on, that can be used as a means of verifying an individual's identity. We use biometric technology to access our smart phones and bank accounts, governments use it to police borders, and companies use it to help ensure that sensitive information is accessed only by authorized individuals.

Some employers use this technology in the form of time clocks that help prevent unauthorized individuals from accessing or changing employee time records. These clocks verify employees' identities when they clock in or out, by scanning a portion of the employee's finger or hand and comparing that with the record of the scan known to be associated with that employee. The clocks do not collect or store an image of the employee's finger or hand; rather, they create and store an encrypted mathematical representation of a portion of the finger or hand. Some states regulate the collection, use, and disclosure of biometric data, which potentially may include the data collected by finger, face or hand scanning time clocks.

How Does ADP Help?

As your compliance partner, we stand ready to assist you in helping to ensure you are meeting your compliance obligations. To this end, we have prepared this toolkit. It includes a summary of major laws which may impact the use of biometric timeclocks as of the date of this publication as well as a model consent form, a model policy and information on how to purge biometric data collected and stored by the time clocks as may be required under the law. We hope that you will find it to be a useful resource.

Legal Landscape

Illinois

To date, the law with the broadest reach is the Illinois Biometric Information Privacy Act ("BIPA"). BIPA requires that companies in possession of biometric data develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric data within a certain period of time. It also requires that companies make certain disclosures and obtain a written release before collecting and storing biometric data, and use a certain standard of care to store, transmit, and protect the data from disclosure.

BIPA allows individuals to file a lawsuit if they believe their rights have been violated. Many lawsuits have been filed against employers operating in Illinois under BIPA, claiming, in general, that the defendants did not obtain consent and provide required notifications before collecting the employees' biometric data.

Courts have not yet determined whether BIPA applies to the data collected by biometric time clocks. But given the risk that BIPA could be found to apply, and the number of lawsuits that have been filed, we are providing the following resources to help you comply with the requirements of BIPA:

- A sample notice / written release to be used before enrolling an employee in the time clock (page 6)
- A sample retention and destruction policy (page 7)
- Information on how to destroy biometric data collected and stored by the time clock. You should purge data when it is no longer needed (*e.g.*, when an employee is no longer employed, or moves to a position that no longer requires use of a timeclock) (page 8).

California

It is a misdemeanor under California law to require an employee or applicant, as a condition of obtaining or securing employment, to furnish his or her fingerprints for the purpose of furnishing that information to a third party, and "these…fingerprints could be used to the detriment of the employee or applicant."

The California Consumer Privacy Act (CCPA) applies to the collection, use, and retention of biometric data. Certain provisions of the CCPA apply to biometric time clocks used to collect employee biometric data, including, among other things, the requirement that, before such collecting biometric data, a business must disclose what information is being collected and the purpose of that collection.

New York

Under New York law, except as otherwise provided by law, employers may not require employees to be fingerprinted as a condition of securing or continuing employment. While the New York State Department of Labor has interpreted this law to prohibit employers from *requiring* employees to use finger scanning technology, employers may request that employees use the technology on a purely voluntary basis.

On the Horizon

Both the federal government and other states are considering laws regulating biometric information. ADP helps clients stay on top of relevant legal developments where the law is fluid and unsettled.

As always, please contact your ADP service representative with whom you normally work if you have any questions.

Sample Consent Forms and Policies

Model Consent Form

Company Name_____ (The "Company")

The employee named below has been advised and understands that the Company, its vendors, and ADP and its vendors, may collect, retain, and use biometric data for the purpose of verifying employee identity and recording time entries if the Company is using biometric timeclocks or timeclock attachments.

Biometric timeclocks are computer-based systems that scan an employee's hand, finger, retina or other physical characteristic and extract unique data points to create a unique mathematical representation. This representation is used to verify the employee's identity, for example, when the employee records their hours worked. The Company's biometric timeclocks do not collect or store images of employees' handprints, fingerprints, retinas or other physical characteristics.

The employee understands that providing biometric data is not required to secure or retain employment and he or she is free to decline to provide biometric data to the Company, its vendors, ADP and its vendors, without any adverse employment action. The employee may revoke this consent at any time by notifying the Company in writing.

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

- 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
- Within 3 years of the employee's last interaction with the Company.

The undersigned employee voluntarily consents to the collection, storage, and use of biometric data through a biometric timeclock as described above. The undersigned employee also voluntarily consents to the Company providing such biometric data to ADP and its vendors for the purposes identified above.

_____

Employee Signature Date

_____

Employee Name (print)

Illinois Sample Biometric Information Privacy Policy

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

Disclosure

The Company will not disclose or disseminate any biometric data to anyone other than its vendors and the licensor of the Company's time and attendance software providing products and services using biometric data 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 and the licensor of the Company's time and attendance software permanently destroy such data when, the first of the following occurs:

- 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
- Within 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.

Removal of Biometric Templates

What are Biometric Templates?

Biometric templates are the data stored in timeclocks and used to verify employee identity for the purpose of recording hours worked. ADP's biometric timeclocks or biometric timeclock attachments do not collect, store, or use actual fingerprints or handprints. Instead, during the enrollment process, the timeclock attachment scans the employee's fingertip or hand, and stores and uses an encrypted mathematical representation of that scan

Why is it Important to Remove Unnecessary Biometric Templates?

In some states in the U.S., notably Illinois, there are laws that regulate the collection, use, and disclosure of certain forms of biometric data, which potentially may apply to the biometric data used in biometric timeclocks. As a best practice, we recommend that organizations remove biometric templates when they are not in use and notify ADP that any biometric templates in ADP's systems be removed, in order to comply with laws that may apply.

Scenario Requiring Removal of Biometric Templates

User Termination

- The user's status changes to terminated within the ADP application - Passed from HR system of record or maintained in ADP Time & Attendance application.
- The employer removes access to the ADP applications.

User Role Change

- The user no longer needs to use a timeclock due to a role change.

User Unable or Refuses to Use Biometric Reader

The user is unable or refuses to use the biometric reader at the clock and your organization agrees to allow Badge or PIN entry as an alternative (note that we advise against forcing employees to use a biometric reader in IL, NY and CA).

Automatic Purge of Biometric Templates

Depending upon the particular model of clock and timekeeping product, biometric templates may be purges automatically at particular intervals. If you have questions about whether your system is configured to automatically purge biometric templates, please contact your ADP service representative

Manual Purge of Biometric Templates

In situations where a system has not been or cannot be configured to delete biometric templates automatically, clients will need to manually purge the templates.

Specific Instructions to Remove Biometric Templates

The process to remove biometric templates is detailed in the User Guide for your particular product. Please consult those materials for specific instructions.

If you have questions about this process, please contact your ADP service representative.

Checklist to Help Support Compliance

Review the requirements on pages 4 and 5.
Ensure that you are using appropriate consent forms and policies as applicable.
Determine a regular schedule for deletion of templates derived from hand or finger scans.
Assign someone in your organization to conduct template deletion on a regular basis and ensure that your deletion practices are consistent with your written policy as applicable.
Contact your ADP representative if you have any questions regarding this process or if you like further information around the storage, maintenance or destruction of biometric data.