KRONOS TIMEKEEPING BIOMETRIC INFORMATION PRIVACY POLICY

In order to efficiently and securely track employees' time records, Alcon Vision, LLC, its affiliates and subsidiaries (collectively, "Alcon") utilizes a biometric timekeeping system, called "Kronos Workforce Dimensions". Alcon has engaged Kronos Incorporated and its affiliated entities providing biometric services ("Vendor") to administer Alcon's timekeeping systems. Consequently, in accordance with applicable provincial / state and federal regulations and other data protection laws, Alcon has instituted the following policy:

Biometric Data Defined

As used in this policy and in simple terms, "*Biometric Data*" means a retina or iris scan, fingerprint, voiceprint, or scan of hand, finger, or face geometry. See the Appendix for more information.

Alcon's Processing of Biometric Data

Alcon and its Vendors collect, store, and use Biometric Data for the purpose of identifying employees and recording time entries when utilizing Alcon's biometric timeclocks or timeclock attachments.

Biometric timeclocks are computer and terminal-based systems that scan an employee's finger or hand for purposes of identification. The computer system used extracts unique data points scanned at the terminal on employee finger tips 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 finger scan data retained from the devices does not contain a fingerprint or image of any kind, but instead consists solely of encrypted or encoded templates with numbers created from mathematical algorithms.

This data is collected, stored, and used solely for employee identification, accurate time-keeping, fraud prevention, and will not be used for any other purpose.

Consent

In order to use the biometric timekeeping system, employees will be asked to sign a consent form authorizing Alcon and/or its Vendor to collect and capture employees' Biometric Data. Employees may choose another method of recording time.

Disclosure

Alcon will not sell, lease, trade, or otherwise profit from an employee's Biometric Data. Nor will it permit Vendor to engage in any such activity. Neither Alcon nor its Vendor will disclose or disseminate an employee's Biometric Data unless authorized to do so by the employee; required to do so by State or federal law; or for other legal compliance reasons.

Retention Schedule

Alcon will retain employee Biometric Data only until, and will request the Vendor permanently destroy such data within one year from the date the first of the following occurs:

a. the initial purpose for collecting or obtaining such Biometric Data has been satisfied, such as the “clocking in/out”, or

b. termination of the employee’s employment with Alcon, or

c. the employee moves to a role within Alcon for which the Biometric Data is not used.

Data Storage, Company Usage, Transmission, and Protection

Alcon will store, transmit, and protect Biometric Data using a reasonable standard of care, and in a manner that is the same as, or more protective than the manner in which Alcon treats other confidential and sensitive information of Alcon and its employees. Biometric Data may be processed by Alcon and Vendor in the following countries:

- Canada
- India
- Ireland
- United States of America

Appendix

- Why does Alcon have this policy?
    - Certain laws require that companies institute policies regarding the processing of Biometric Data, such as the Illinois Biometric Information Privacy Act, the Texas Biometric Privacy Law, the General Data Protection Regulation, and other provincial/state and federal regulations.

- Is "Biometric Data" only a retina or iris scan, fingerprint, voiceprint, or scan of hand, finger, or face geometry?
    - No. Biometric Data may also consist of other personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a person, which allow or confirm the unique identification of that person such as 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 are not within the scope of this Policy and Consent. Also excluded are 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 US federal Health Insurance Portability and Accountability Act of 1996 or other applicable laws that specifically address the use of medical information.

- Tell me more about when this Biometric Data may be disclosed by Alcon or the Vendor.
    - Alcon or the Vendor may further disclose or disseminate the Biometric Data if: 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.

- How will the Biometric Data be destroyed?

    Biometric Data will be destroyed during a periodic review by the system architect in which biometric scans will be removed from the Kronos Touch ID options at the clock and the database. An authorized Alcon system administrator will perform a process which permanently deletes the biometric scan stored at the clock and the database.