Accurate Biometrics, Inc.

Retention and Destruction Policy

For

Identifiers and Other Biometric Information

Updated: September 4, 2020

Accurate Biometrics, Inc.
500 Park Boulevard
Suite 1260
Itasca, Illinois 60143
Phone: (866) 361-9944

IDFPR Live Scan Fingerprint Provider
Agency License #262.000016

Section 1. Introduction

1.1. Background

Section 1240.535(c)(8) of the Illinois Administrative Code regulating fingerprint vendors provides: “A licensed fingerprint vendor must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying identifiers and other biometric information when the initial purpose for collecting or obtaining the identifiers or information has been satisfied or after 3 years from the individual's last interaction with the licensed fingerprint vendor, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines” (the “Regulation”). This Policy is drafted pursuant to the Regulation and the Act (defined below).

1.2 Definitions

The above language in the Regulation appears to be based upon language in the Illinois Biometric Information Privacy Act found at 740 ILCS 14/ (the “Act”). The terms "identifiers" and "biometric information" are not defined by the Regulation; however the terms “biometric identifier" and “biometric information” are defined in the Act and will be used to construe the term "identifiers and other biometric information" in the Regulation. Accordingly, whenever used within this Policy, unless otherwise clearly documented:

(a) "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.

(b) "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.

(c) "Identifiers and other biometric information" means biometric identifiers and biometric information.

Section 2. Retention Policy

2.1 Retention

Unless obligated by customer contract or the "FBI CJIS Security Policy" to maintain fingerprint images for a specific period of time, all identifiers and other biometric information, including fingerprint images will be retained for up to 90 days from the date of receipt, fingerprint capture or card scan date, or the "date last modified", in the case where the original fingerprint or card scan date was modified. Exhibit A (available upon request) is part of this policy and contains an updated list of customer contract categories or names listing retention policies that differ from the above 90 days. Exhibit A will be updated from time to time. If a fatal or non-fatal error occurs requiring the re-transmission of fingerprint images, the "date last modified" will be updated, beginning a new 90-day retention period. 90 days is a proper retention period as it allows for the resubmission of prints for customers and applicants who either do not receive reports or accidentally misplace reports they have received. The 90-day period also prevents inconveniencing the fingerprinted applicant as they do not need to be re-printed if reports are lost or not received.

When an error results in the need for a new set of fingerprint images to be taken, this creates a new fingerprint inquiry transaction with a new date of fingerprint capture, starting the 90 day retention date from the revised date of fingerprint capture.

When obligated by customer contract or the "FBI CJIS Security Policy" to retain fingerprint images for a specific period of time other than 90 days, Accurate Biometrics has electronically programmed its retention database to retain the digital images to the specific requesting agency requirements. Electronic retention has been built utilizing the purpose for which the fingerprints were captured, in addition to the requesting agency Originating Agency Identifier assigned by the Illinois State Police, Bureau of Identification or the Federal Bureau of Investigation.

Accurate Biometrics recognizes there may appear to be a conflict between the Regulation and the requirements with respect to certain contracts with respect to the retention time frame, but believes the intent of the Regulation is not to conflict with governmental contractual requirements and can be reconciled by the fact that the initial purpose of the contractual requirement has not been met and the governmental entity is relying upon the fingerprinting agency for archival of its records. Additionally, the Act specifically provides that it does not apply to contractors of State or local governments and this further supports that the Regulations are not intended to restrict a government contractor from retaining records longer than 3 years. Therefore, a period of retention of greater than 3 years is warranted in certain circumstances.

2.2 Retention of Employee Records

The identifiers and other biometric information maintained on Accurate Biometric employees will be maintained by Accurate Biometrics for the duration of employment with the company except that fingerprint records shall be kept only for the time required to obtain the applicable report from the applicable agency and will be deleted after receipt of such report.

Section 3. Permanent Destruction Policy

Section 3.1 Electronic Documents

Once the Record Retention Schedule has been met, a secure electronic "delete" function takes place. Immediately after the secure "delete" function takes place, the identifiers and other biometric information are no longer accessible and permanently destroyed on the applicable hard drive. Understanding that the standard "delete" function by itself in today's digital arena, is not sufficient to permanently "destroy" these electronic documents, the following steps are also put into place, to ensure the data is not recoverable.

In order to protect the privacy and confidentiality and recoverability of our captured data and in order to be in compliance with the FBI CJIS Security Policy and related requirements, Accurate Biometrics has a policy in place to ensure hard drives are backed up on other hard drives in case there is a hard drive failure. Such hard drives are encrypted and only to be used to restore data that has been lost. Once the archival period for a hard drive has expired, Accurate Biometrics completely erases and overwrites all data stored on each hard drive and then physically destroys the hard drive. Accurate Biometrics hires a certified third party to "shred" such hard drives in order to securely destroy the physical hardware. Upon completion of the hard drive "shred", Accurate Biometrics receives an official signed shred certificate.

Section 3.2 Physical Documents

Some identifiers and other biometric information may be received in paper form, e.g. fingerprint cards. Such Identifiers and other biometric information are converted into an electronic/digital format. Thereafter the physical documents are placed in a file for a period of up to 30 days. On or before such 30 days expires, the physical documents are placed in a secure shred bin. On a bi-monthly basis, a third party hired by Accurate Biometrics, securely shreds the contents of the shred bins.

Section 3.3 Employee Files

Once an employee has terminated employment with the company, all other biometric information will be destroyed following the policies in Sections 3.1 and 3.2 subject to any retention requirements in applicable law.

Section 4. Exceptions to Policy

Absent a valid warrant or subpoena issued by a court of competent jurisdiction or other applicable law or legal requirement, Accurate Biometrics will comply with the Policy.

Section 5. Roles and Responsibilities

Accurate Biometrics has assigned its President to be responsible for overseeing and implementing the Policy.

Section 6. Questions and Copies

This Policy shall be available to the public and be provided upon request. Questions related to the Policy, including requests for the most recent version of the Policy, should be directed to:

Attn: President
Accurate Biometrics, Inc.
500 Park Boulevard
Suite 1260
Itasca, Illinois 60143
e-Mail: privacy@accuratebiometrics.com