FIRM Systems

Illinois Licensed Fingerprint Vendor

Agency License: 262.000011

Biometrics Retention and Destruction Policy

Updated April 15th 2022

Section 1. Introduction

Futures in Rehabilitation Management dba FIRM Systems ("FIRM Systems") is an Illinois headquartered licensed fingerprint vendor. 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 in order to inform fingerprint applicants about how FIRM Systems handles, stores and processes certain applicant information. This Policy will be periodically updated, and you can receive the most recent version by emailing: info@firmsystems.net.

Section 2. Retention Policy

All identifiers and other biometric information, including fingerprint images will be retained on the local device for no longer than 30 days. All identifiers and other biometric information including fingerprint images will be retained on the FIRM Systems Headquarters' server for a period no longer than 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. If a fatal or non-fatal error occurs requiring the retransmission 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 fingerprints 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 fingerprint applicant as they do not need to be reprinted 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.

Section3. Permanent Destruction Policy

Section 3.1 Electronic Documents

All identifiers and other biometric information which are stored electronically are permanently deleted once 90 days have passed.

Section 3.2 Physical Documents

Some identifiers and other biometric information may be received in paper form, i.e. 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 FIRM Systems, securely shreds the contents of the shred bins.

Section 4. Exceptions to the Policy

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

Section 5. Roles and Responsibilities

FIRM Systems has assigned its President to be responsible for overseeing and implementing the Policy.

Section 6. Definitions

The terms "identifiers" and "biometric information" are not defined by the Regulation; however, the terms “biometric identifier" and “biometric information” are defined in the Illinois Biometric Information Privacy Act found at 740 ILCS 14/ (the “Act”) and such definitions are applied in this Policy. 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.
(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 7. 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

FIRM Systems, Inc.

6 Lawrence Sq

Springfield, IL 62704

e-mail: info@firmsystems.net