

12.15.05.00

# **Title 12 DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES**

## **Subtitle 15 CRIMINAL JUSTICE INFORMATION SYSTEM CENTRAL REPOSITORY**

### **Chapter 05 Use of Private Provider Services for Non-Criminal Justice Purposes**

**Authority: Criminal Procedure Article, §10-221, Annotated Code of Maryland**

*12.15.05.01*

**.01 Purpose.**

This chapter establishes minimum requirements and procedures for a private provider to perform fingerprinting services and demographic data collection for non-criminal justice purposes for the Central Repository.

12.15.05.02

## **.02 Definitions.**

A. In this chapter, the following terms have the meanings indicated.

B. Terms Defined.

- (1) "Authorization certificate" means a document issued by the Central Repository to a private provider authorizing the private provider to perform fingerprinting services and demographic data collection for the Central Repository.
- (2) "Criminal history records check" has the meaning stated in COMAR 12.15.02.02.
- (3) "Criminal history record information (CHRI)" has the meaning stated in Criminal Procedure Article, §10-201(d), Annotated Code of Maryland.
- (4) "Criminal Justice Information System—Central Repository (Central Repository)" has the meaning stated in Criminal Procedure Article, §10-201(c), Annotated Code of Maryland.
- (5) "Criminal justice purposes" has the meaning stated in COMAR 12.15.01.03.
- (6) "FBI" means the United States Federal Bureau of Investigation.
- (7) "Network Livescan Applicant Technical Interface Document" means the written minimum specifications for processing a request for a criminal history records check for non-criminal justice purposes.
- (8) "Non-criminal justice purpose" means the use of criminal history record information for licensing and employment purposes.
- (9) "Private provider" means a person performing fingerprinting services and demographic data collection for non-criminal justice purposes.
- (10) "Private provider agreement" means a legally binding document that describes the responsibilities of the Central Repository and a private provider authorizing the private provider to perform fingerprinting services and demographic data collection for the Central Repository.
- (11) "Record" means any printed, written, or electronic document or file used or created for the purposes of collecting and transmitting fingerprint images and demographic data to the Central Repository for a request for a criminal history records check for non-criminal justice purposes.

12.15.05.03

### **.03 Private Provider Performing Fingerprinting Services and Demographic Data Collection.**

A. The Central Repository may authorize a private provider to perform fingerprinting services and demographic data collection for a request for a criminal history records check for non-criminal justice purposes.

B. The Central Repository shall establish minimum administrative and operational requirements for private providers to perform fingerprinting services and demographic data collection for non-criminal justice purposes.

C. Fingerprinting services and demographic data collection for non-criminal justice purposes include:

(1) Electronic transmission of an individual's fingerprints and demographic data to the Central Repository for a criminal history records check for non-criminal justice purposes;

(2) Completion of forms required for a request for a criminal history records check by obtaining information about the individual being fingerprinted; and

(3) Collection of fees and payment of invoices according to Regulation .07 of this chapter.

D. Except for purposes under §E of this regulation, a private provider authorized to perform fingerprinting services and demographic data collection for non-criminal justice purposes under this chapter shall make the private provider's fingerprinting services available to a person requesting a criminal history records check for non-criminal justice purposes.

E. A private provider may not perform fingerprinting services or demographic data collection for the following purposes:

(1) Sex offender registration;

(2) Hazardous materials endorsements—commercial driver's licenses; or

(3) Criminal justice purposes.

12.15.05.04

#### **.04 Private Provider Agreement and Authorization Certificate.**

A. A private provider may not provide fingerprinting services or demographic data collection for non-criminal justice purposes unless the private provider meets requirements under this chapter.

B. Before the Central Repository enters into a private provider agreement with or issues an authorization certificate, original or renewal, to a private provider requesting to perform fingerprinting and demographic data collection under this chapter, the private provider shall:

(1) Submit a written application to the Central Repository in a format established by the Central Repository;

(2) Provide the Central Repository with documents indicating that the private provider has been providing fingerprinting services and demographic data collection for at least 5 years immediately preceding application;

(3) Demonstrate the ability to electronically transmit fingerprint images and demographic data using a secure encrypted connection that meets requirements set forth in the Network Livescan Applicant Technical Interface Document maintained by the Central Repository;

(4) Demonstrate compliance with requirements under Regulation .05 of this chapter for the location where Central Repository authorized fingerprinting services and demographic data collection are performed;

(5) Provide documents to support the existence of a current surety bond as provided under Regulation .09 of this chapter; and

(6) Demonstrate that a criminal history records check was performed on the private provider's employee as required under Regulation .08 of this chapter.

C. The Central Repository shall issue an Authorization Certificate to a private party meeting the requirements of this chapter that:

(1) Is valid for 2 years from the date of issuance, unless suspended by the Central Repository; and

(2) May be renewed every 2 years upon application by a private provider, unless the Central Repository has suspended the authorization certificate.

D. A private provider shall notify the Central Repository within 10 business days of a change in the information submitted as part of an original or renewal application under this chapter.

E. A private provider issued an authorization certificate under this chapter shall display the certificate at the location where the fingerprinting services and demographic data collection are performed.

12.15.05.05

### **.05 Private Provider Business Location Requirements.**

A. Before the Central Repository enters into a private provider agreement with or issues an original or renewal authorization certificate to a private provider, the Central Repository shall review a private provider's location plan.

B. A private provider's location plan, at a minimum, shall have:

- (1) A Livescan machine that is approved by the Central Repository;
- (2) A waiting area that, at a minimum, includes:
  - (a) A reception desk; and
  - (b) Seating for individuals requesting a criminal history records check;
- (3) A method of securing and maintaining records that meets Central Repository requirements;
- (4) A dedicated telephone line used exclusively for private provider communication with the Central Repository; and
- (5) Electronic connections, electric power supply, and office climate control that meet manufacturer and Central Repository requirements.

12.15.05.06

## **.06 Records.**

A. A private provider authorized to perform fingerprinting services and demographic data collection under this chapter shall:

- (1) Retain records related to a request for a criminal history records check for 90 days from the date of the request; and
- (2) Then destroy the records.

B. Records, at a minimum, include the following for the individual being fingerprinted and supplying demographic data:

- (1) An identification number;
- (2) The name and address;
- (3) The date that the individual was fingerprinted and provided the demographic data;
- (4) A copy of driver's license or other acceptable identification;
- (5) The processing control number;
- (6) The fingerprint image;
- (7) The type of transaction;
- (8) The authorization number;
- (9) The matrix code associated with transaction;
- (10) A record of fees collected; and
- (11) A record of payment to the Central Repository.

C. A private provider shall ensure confidentiality of records that are stored and destroyed according to requirements of this chapter.

D. Records are subject to inspection by the Central Repository or the FBI.

E. A private provider may not receive criminal history records check information.

12.15.05.07

**.07 Fees.**

A. A private provider shall collect fees as specified under COMAR 12.15.01.14 for performing fingerprinting services and demographic data collection for non-criminal justice purposes on behalf of the Central Repository.

B. The Central Repository shall submit a monthly invoice to each private provider for requests for criminal history records checks processed by the private provider and submitted to the Central Repository during the preceding month.

C. Upon receipt of the invoice under §B of this regulation, the private provider shall forward payment to the Central Repository within 7 business days of receipt of invoice.

D. A private provider may charge fees for providing fingerprinting services and demographic data collection in addition to fees as specified under COMAR 12.15.01.14.

E. If a private provider charges fees in addition to those required under COMAR 12.15.01.14, the private provider shall:

(1) Identify, report, and control the additional fees separately from those required to be collected by the Central Repository under COMAR 12.15.01.14; and

(2) Include in any public notice of the availability of fingerprinting and demographic data collection for non-criminal justice purposes:

(a) The fees required under COMAR 12.15.01.14; and

(b) The additional fees charged by the private provider.



12.15.05.08

**.08 Criminal History Records Check for Private Provider Employees.**

A. As part of the application for an original or renewal authorization certificate, a private provider shall include the fingerprints and demographic data for each individual performing or supervising fingerprinting services and demographic data collection authorized under this chapter.

B. The Central Repository shall conduct a criminal history records check of each individual identified by the private provider as performing or supervising fingerprinting services or demographic data collection authorized under this chapter.

C. The Central Repository may consider CHRI received under §B of this regulation when determining:

(1) Whether to authorize a private provider to perform fingerprinting services and demographic data collection under this chapter; or

(2) The conditions of the private provider agreement.

12.15.05.09

**.09 Surety Bond.**

A. A private provider requesting authorization to perform fingerprinting services and demographic data collection for non-criminal justice purposes shall have a surety bond of \$10,000, in a form approved by the Central Repository.

B. A private provider shall provide the Central Repository with:

(1) A certificate from the bonding company listing the individuals of the private provider's company who are covered by the bond;

(2) An agreement from the bonding company that the bonding company shall give the Central Repository at least 45 days notice by registered or certified mail of cancellation of the private provider's bond; and

(3) As part of the agreement under §B(2) of this regulation, written assurance that the bond will be in full force and effect for a period of at least 45 days after notice of cancellation is given to the Central Repository.

C. After an original or renewal authorization certificate is issued, the private provider shall maintain the required surety bond throughout the period the private provider is authorized to perform fingerprinting services and demographic data collection for non-criminal justice purposes under this chapter.

12.15.05.10

## **.10 Suspension of an Authorization Certificate.**

A. The Central Repository may suspend an authorization certificate granted under this chapter, if the Central Repository determines that the private provider:

(1) Perpetrated a fraud against the Central Repository or the public;

(2) Created the impression that the private provider is associated with or is a part of the Central Repository or another State agency;

(3) Conducted business in a manner that is detrimental to the interests of the Central Repository, the State, or the public;

(4) Has not met the administrative or operational requirements for authorization under this chapter;

(5) Has more than a 2 percent rejection rate of fingerprint impressions as determined by the Central Repository or FBI;

or

(6) Failed to forward payments to the Central Repository as required under this chapter.

B. The private provider may reapply for an authorization certificate after 6 months from the date of a suspension.