**299C.40 COMPREHENSIVE INCIDENT-BASED REPORTING SYSTEM.**

Subdivision 1. **Definitions.** (a) The definitions in this subdivision apply to this section.

(b) "CIBRS" means the Comprehensive Incident-Based Reporting System, located in the Department of Public Safety and managed by the Bureau of Criminal Apprehension, Criminal Justice Information Systems Section. A reference in this section to "CIBRS" includes the Bureau of Criminal Apprehension.

(c) "Law enforcement agency" means a Minnesota municipal police department, the Metropolitan Transit Police, the Metropolitan Airports Police, the University of Minnesota Police Department, the Department of Corrections Fugitive Apprehension Unit, a Minnesota county sheriff's department, the Bureau of Criminal Apprehension, or the Minnesota State Patrol.

Subd. 2. **Purpose.** CIBRS is a statewide system containing data from law enforcement agencies. Data in CIBRS must be made available to law enforcement agencies in order to prepare a case against a person, whether known or unknown, for the commission of a crime or other offense for which the agency has investigative authority, or for purposes of background investigations required by section 626.87.

Subd. 3. **Data practices act governs.** The provisions of chapter 13 apply to this section.

Subd. 4. **Data classification; general rule; changes in classification; audit trail.** (a) The classification of data in the law enforcement agency does not change after the data is submitted to CIBRS. If CIBRS is the only source of data made public by section 13.82, subdivisions 2, 3, 6, and 7, data described in those subdivisions must be downloaded and made available to the public as required by section 13.03.

(b) Data on individuals created, collected, received, maintained, or disseminated by CIBRS is classified as confidential data on individuals as defined in section 13.02, subdivision 3, and becomes private data on individuals as defined in section 13.02, subdivision 12, as provided by this section.

(c) Data not on individuals created, collected, received, maintained, or disseminated by CIBRS is classified as protected nonpublic data as defined in section 13.02, subdivision 13, and becomes nonpublic data as defined in section 13.02, subdivision 9, as provided by this section.

(d) Confidential or protected nonpublic data created, collected, received, maintained, or disseminated by CIBRS must automatically change classification from confidential data to private data or from protected nonpublic data to nonpublic data on the earlier of the following dates:

(1) upon receipt by CIBRS of notice from a law enforcement agency that an investigation has become inactive; or

(2) when the data has not been updated by the law enforcement agency that submitted it for a period of 120 days.

(e) For the purposes of this section, an investigation becomes inactive upon the occurrence of any of the events listed in section 13.82, subdivision 7, clauses (a) to (c).

(f) Ten days before making a data classification change because data has not been updated, CIBRS must notify the law enforcement agency that submitted the data that a classification change will be made on the 120th day. The notification must inform the law enforcement agency that the data will retain its classification as confidential or protected nonpublic data if the law enforcement agency updates the data or notifies CIBRS that the investigation is still active before the 120th day. A new 120-day period begins if the data is updated or if a law enforcement agency notifies CIBRS that an active investigation is continuing.

(g) A law enforcement agency that submits data to CIBRS must notify CIBRS if an investigation has become inactive so that the data is classified as private data or nonpublic data. The law enforcement agency must provide this notice to CIBRS within ten days after an investigation becomes inactive.

(h) All queries and responses and all actions in which data is submitted to CIBRS, changes classification, or is disseminated by CIBRS to any law enforcement agency must be recorded in the CIBRS audit trail.

Subd. 5. **Access to CIBRS data by law enforcement agency personnel.** Only law enforcement agency personnel with certification from the Bureau of Criminal Apprehension may enter, update, or access CIBRS data. The ability of particular law enforcement agency personnel to enter, update, or access CIBRS data must be limited through the use of purpose codes that correspond to the official duties and training level of the personnel.

Subd. 6. **Access to CIBRS data by data subject.** (a) Upon request to the Bureau of Criminal Apprehension or to a law enforcement agency participating in CIBRS an individual shall be informed whether the individual is the subject of private or confidential data held by CIBRS. An individual who is the subject of private data held by CIBRS may obtain access to the data by making a request to the Bureau of Criminal Apprehension or to a participating law enforcement agency. Private data provided to the subject under this subdivision must also include the name of the law enforcement agency that submitted the data to CIBRS and the name, telephone number, and address of the responsible authority for the data.

(b) If an individual who is the subject of private data held by CIBRS requests access to the data or release of the data to a third party, the individual must appear in person at the Bureau of

Criminal Apprehension or a participating law enforcement agency to give informed consent to the data access or release.

Subd. 7. **Challenge to completeness and accuracy of data.** An individual who is the subject of public or private data held by CIBRS and who wants to challenge the completeness or accuracy of the data under section 13.04, subdivision 4, must notify in writing the responsible authority for the data. A law enforcement agency must notify the Bureau of Criminal Apprehension when data held by CIBRS is challenged. The notification must identify the data that was challenged and the subject of the data. CIBRS must include any notification received under this paragraph whenever disseminating data about which no determination has been made. When the responsible authority of a law enforcement agency completes, corrects, or destroys successfully challenged data, the corrected data must be submitted to CIBRS and any future dissemination must be of the corrected data.

**History:** *2005 c 163 s 81; 2006 c 253 s 16,17; 2006 c 260 art 3 s 14*