



COMMISSIONER
Adelaide Horn

March 24, 2009

To: All Licensed Providers Covered by Health & Safety Code (H&SC) Chapter 250 (Assisted Living Facilities, Adult Day Care Facilities, Home and Community Support Service Agencies, Licensed Intermediate Care Facilities for Persons with Mental Retardation or Related Conditions and Nursing Facilities)

Subject: **Provider Letter 09-05** – Surveyor Review of Department of Public Safety (DPS) Criminal History Reports Retrieved from the DPS Secure Website
(Replaces PL 08-19)

Because of some recent instances of providers declining to allow surveyors to review employee criminal history reports, the Department of Aging and Disability Services (DADS) is issuing this letter to provide guidance and clarification related to the review of DPS criminal history reports by DADS Regulatory Services surveyors.

In general, DPS criminal history reports retrieved by providers from the DPS secure website are confidential and are intended for the exclusive use of the requesting provider (H&SC §250.007). H&SC §§250.007 and 250.008 and Government Code §411.085 prohibit providers from disclosing criminal history reports to individuals who are not entitled to the information. DPS, through its Non-Criminal Justice Audit and Training unit, has begun training and auditing users of the DPS secure website. DPS is enforcing stringent user compliance with the statutory provisions related to confidentiality and compliance with the DPS-mandated information security policy. The DPS security policy is provided as an attachment to this memo. The providers who declined to allow surveyors to review employee criminal history reports stated that they did so in the context of complying with DPS mandates.

DADS, as a regulatory agency, is entitled by H&SC §250.002(a) and Government Code §411.1387 to obtain criminal history information from DPS. DPS defines access to criminal history information as the ability to receive, view or discuss criminal history record information regardless of the retrieval method. DPS agrees that surveyors, while on site, may review the confidential criminal history reports that providers have retrieved from the DPS secure website. If, during a survey or investigation, a surveyor needs to retain a particular criminal history report, the surveyor will obtain a copy from DPS.

The DPS Audit and Training unit, in future training sessions and audits of users of the secure website, will be informing users that they may allow DADS surveyors to review criminal history reports that have been retrieved from the DPS secure site.

Also attached is a sample criminal history document log. The H&SC and the Texas Administrative Code do not require providers to use this log. This is a sample of a tool that may be used for the tracking and disposition of criminal history checks.

Provider Letter #09-05
March 24, 2009
Page 2

If you have questions regarding the content of this memo, please contact a policy specialist in the Policy, Rules and Curriculum Development unit at 512-438-3161.

Sincerely,

[signature on file]

Veronda L. Durden
Assistant Commissioner
Regulatory Services

VLD:ca

Attachments

TEXAS DEPARTMENT OF PUBLIC SAFETY

SECURITY POLICY FOR NON-CRIMINAL JUSTICE AGENCIES' ACCESS, USE, AND DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

I. ACCESS BY NONCRIMINAL JUSTICE ENTITIES

A. Legislative Authority for Non-criminal Justice Entities' Access

Policy: A non-criminal justice entity legislatively authorized by Chapter 411, Subchapter F of the Texas Government Code or other Texas law to receive criminal history record information (CHRI) from the Department of Public Safety (Department) may access the DPS databases. All non-criminal justice entities granted access to the DPS CHRI will be subject to all applicable state and federal laws, rules, regulations and policies that relate to the obtaining, use and dissemination of CHRI.

The Federal Bureau of Investigation (FBI) may authorize certain Texas entities access to FBI criminal history record information based upon approved Texas statutes or federal law.

Commentary: All DPS databases are maintained by the Department and may be accessed pursuant to Chapter 411, Subchapter F of the Texas Government Code or other Texas law. A non-criminal justice entity granted access to the DPS databases may submit criminal history inquiries through the DPS Access and Dissemination Bureau, Criminal History Inquiry Unit, through the DPS Secure Website for Criminal History Information, through fingerprint submission. Results will be provided on-line through the DPS Secure Website, through the Fingerprint-based Applicant Clearinghouse of Texas (FACT), via the mail, or through other means, as agreed upon between DPS and the requestor. The DPS databases will provide a non-criminal justice entity only with CHRI originating in Texas. In those instances where fingerprints are submitted under a statute approved for access to the FBI records, DPS will forward the fingerprints to the FBI and FBI will provide the record response through the DPS.

B. Non-criminal Justice Entity User Agreements

Policy: A non-criminal justice entity requesting access to the DPS databases must provide the Department with a signed written user agreement in which the entity agrees to comply with Department policies regarding the use of the DPS databases or information. The user agreement will include standards and sanctions governing the non-criminal justice entity's utilization of the DPS databases or information and will incorporate the policies set forth in this document. These policies also apply to access to, use, and dissemination of FBI criminal history record information, when appropriate.

Commentary: None

II. PERSONNEL SECURITY

A. Authorized Users

Policy: A non-criminal justice entity must provide the Department with the name, sex, race, date of birth, and title of each official/employee of the non-criminal justice entity who will utilize information received from the DPS databases. The Department will perform a name-based background check on each name submitted, and reserves the right to require a fingerprint-based background check, prior to approving access for the official/employee. Only those persons approved by the Department, herein after referred to as authorized employees, will be allowed access to the DPS databases or information on behalf of the non-criminal justice entity. An official/employee who is not approved to utilize the DPS databases or information may dispute the information forming the basis of the Department's decision through the submission of fingerprints. The Department may limit the number of authorized employees within a non-criminal justice entity. These same personnel screening criteria apply to access to the FBI criminal history record information received from FBI through the DPS.

Commentary: Only authorized users may access the information received from the DPS and FBI databases. The number of authorized users shall be limited to the number reasonably necessary to perform criminal history checks for the purposes permitted by law.

B. User Identifier

Policy: A Department-issued user entity identifier shall be used in each transaction in the DPS databases for retrieval of CHRI.

Commentary: The Department will assign a user identifier to each non-criminal justice entity authorized by the Department to access the DPS databases for CHRI. This user identifier serves to identify the non-criminal justice entity accessing the DPS and FBI databases and ensures the proper level of access for the non-criminal justice entity.

III. FACILITY AND INFORMATION SECURITY

A. Facility Security Standards

Policy: The location of all CHRI received from the DPS or FBI databases must have adequate physical security to protect against any unauthorized viewing or access to displayed/stored/printed criminal history record information at all times.

Commentary: File cabinets or file systems used to maintain CHRI must be protected from unauthorized viewing of or access to CHRI. For example, either locking of the file cabinet or locking the access to the room the files are housed is one component of complying with this policy.

B. Information Security Standards

Policy: Criminal history record information obtained from the DPS or FBI databases is sensitive information and must be maintained in a secure records environment to prevent the unauthorized viewing or use of the criminal history record information.

Commentary: None

Policy: When retention of criminal history record information is no longer necessary or is not permitted by law, the criminal history record information shall be properly disposed. A secure manner of disposal must be utilized to destroy thoroughly all elements of the records and preclude unauthorized viewing, access or use.

Commentary: Disposal procedures should include a method sufficient to preclude recognition or reconstruction of information (i.e., shredding). The method should also provide verification that the disposal procedures were successfully completed.

IV. CRIMINAL HISTORY RECORD INFORMATION

A. Obtaining, Use and Dissemination of Criminal History Record Information

Policy: A non-criminal justice entity may retrieve criminal history record information through the DPS or FBI databases only for legislatively authorized purposes. Criminal history record information received from the DPS or FBI databases shall be used only for legislatively authorized purposes and may not be disseminated to a person not authorized to receive the information. Upon request by the Department, all users must provide an authorized purpose for all criminal history record information inquiries. The ability to retrieve criminal history record information is subject to cancellation if the information is obtained or used in an unauthorized manner or disseminated to a person not authorized to receive the criminal history record information. Criminal sanctions are also in place for the improper obtaining, use and dissemination of criminal history record information.

Commentary: Generally, criminal history record information held by the DPS and the FBI is confidential and may be disseminated only as authorized by state or federal statute. Specific non-criminal justice entities are legislatively authorized to receive criminal history record information for limited, specified purposes. The non-criminal justice entity is responsible for complying with all laws governing the non-criminal justice entity's access to, use, and dissemination of criminal history record information. State law makes it unlawful for a person to obtain confidential criminal history record information in an unauthorized manner, use the information for an unauthorized purpose, or disclose the information to a person not entitled to the information. State law also makes it unlawful for a non-criminal justice entity to provide a person with a copy of the person's criminal history record information obtained from the Department unless authorized to do so by a specific state statute.

B. Commercial Dissemination

Policy: The commercial dissemination of criminal history record information obtained through the DPS databases is prohibited.

Commentary: The marketing of data for profit is not permitted. State law makes it a felony offense to obtain, use, or disclose, or employ an other to obtain, use or disclose, criminal history record information for remuneration or for the promise of remuneration.

V. AUDITS

Security Audits

Policy: A security audit may be performed on a periodic basis by the Department for the purpose of measuring the non-criminal justice entity's compliance with the laws, rules, regulations and policies relating to the DPS databases and the criminal history record information obtained therefrom.

