



University of Pennsylvania Police Department 4040 Chestnut Street, Philadelphia, Pa 19104		 
Directive: 44	Subject: Criminal Intelligence and Dissemination of Protected Information	Effective Date: 05/26/1998
Order of: Gary Williams, Chief of Police		Amended Date: 08/01/2023

I. Purpose

The purpose of this directive is to establish policy guidelines for the University of Pennsylvania Police Department (UPPD) which will enable this department to gather, disseminate, and receive intelligence, investigative and treatment data from other conforming criminal justice agencies. This data being classified as "protected information" by 18 Pa. C.S.A. section 9106.

II. Policy

It is policy of the UPPD to conform to the mandates of the Criminal History Record Information Act 18 Pa. C.S.A. section 9106 et.seq. (CHRIA). Additionally, all members of the department, who receive information relative to suspicious incidents, criminal incidents, and activities which could be a potential threat to homeland security will report such activities through their chain of command in a timely manner.

III. Scope

This directive shall affect all UPPD employees.

IV. Definitions

- A. Automated Systems: A computer or other internally programmed device capable of automatically accepting and processing data, including computer programs, data communication links, input and output data and data storage devices.
- B. Criminal History Agency: A court, including the minor judiciary, with criminal jurisdiction or another governmental agency, or sub-unit thereof, created by statute or by the State or Federal Constitution, specifically authorized to perform as its principal function the administration of criminal justice, and which allocates a substantial portion of its annual budget to that function. The term includes organized state and municipal police departments, local detention facilities, county, regional and state correction facilities; probation agencies; district and prosecuting attorneys; parole boards; pardon boards and agencies or sub-units thereof, as are declared by

the Attorney General to be criminal justice agencies as determined by a review of applicable statutes and the State and Federal Constitution, or both.

- C. Protected Information: -intelligence, investigative or treatment information.
 - 1. Intelligence Information: Information concerning the habits, practices, characteristics, possessions associations or financial status of an individual compiled in an effort to anticipate, prevent, monitor, investigate or prosecute criminal activity.
 - 2. Investigative Information: Information assembled as a result of the performance of an inquiry, formal or informal, into a criminal incident or an allegation of criminal wrongdoing and may include modus operandi information.
 - 3. Treatment Information: Information concerning medical, psychiatric, psychological, or other rehabilitative treatment provided, suggested or prescribed for an individual charged with or convicted of a crime.
- D. Repository: A location in which history record information is collected, compiled, maintained and disseminated by a criminal justice agency.
- E. Central Repository: The central location for the collection, compilation, maintenance and dissemination of criminal history record information by the Pennsylvania State Police.
- F. Criminal History Record Information: Information collected by criminal justice agencies concerning individuals, and arising from the initiation of the criminal proceeding, consisting of identifiable descriptions, dates and notations of arrests, indictments, information or other formal criminal charges and dispositions arising therefrom. The term does not include intelligence, information, investigative information or treatment information, including medical and psychological information or information and records specified in 18 Pa. C.S.A. section 9104 (relating to scope).

V. Procedures

- A. Intelligence Officer
 - 1. The Deputy Chief of Investigations will be designated as the intelligence officer for the UPPD and will be responsible for the classification, computerization and dissemination of all intelligence information, as well as all "protected information" classified in CHRIA. He/she may designate other members of the UPPD to perform this duty on an as needed basis upon approval of the Chief of Police.
 - 2. Intelligence-related documentation may include, but not be limited to, police reports submitted and prepared by officers of the UPPD; police reports from federal, state and local law enforcement agencies, e-mail, meeting minutes and any other written documentation that meets the criteria of criminal intelligence information as defined within this directive.

B. Collection of Intelligence Information

1. The department will collect and securely store intelligence information ONLY when the following conditions are met:
 - a. The information concerns an individual or group which it reasonably suspects of criminal activity.
 - b. The information is related to criminal activity that would give rise to prosecution for a state offense graded a misdemeanor or felony or for a Federal offense for which a penalty is imprisonment for more than one year.
 - c. The information is categorized based upon subject matter.
 - d. The information does not concern participation in a political, religious or social organization, or in the organization or support of a nonviolent demonstration, assembly, protest, rally or similar form of public speech, unless there is a reasonable suspicion that the participation by the subject of the information is related to criminal activity or prison rule violation.
 - e. The intelligence information is not collected in violation of state law.
 - f. The information collected relates to activities that present a potential threat to the UPPD's jurisdiction.
2. Intelligence information will not be collected for, or transferred to the central repository maintained by the Pennsylvania State Police.

C. Security of Protected Information

1. The confidentiality of protected information will be provided for and securely maintained by:
 - a. Following **Directive 17, "UPPD Building Security Regulations,"** to reasonably protect repository from theft, sabotage and man-made or natural disasters.
 - b. Properly selecting, supervising, and training personnel authorized to have access to protected information.
 - c. Insuring that, where computerized data processing is employed, the equipment utilized for maintaining intelligence information, investigative information or treatment information is dedicated solely to purposes related to the administration of criminal justice. If the equipment is not used solely for the administration of criminal justice, the criminal justice agency is accorded equal management participation in computer information or treatment information.

- d. Insuring that only those authorized to access protected information are electronically coded or otherwise designated to enter the automated system. The intelligence officer will maintain a copy of the authorization list.
- e. Three different levels of storage of protected information will be established for reliability and sensitivity:

Level 1: Will include all information that has been received from a reliable source and is substantiated.

Level 2: Will include all information that has been received from a reliable source but is unsubstantiated.

Level 3: Will include all information that has been received from an unreliable source and is not and cannot be substantiated.

D. Safeguarding, Securing and Storing of Criminal Intelligence Information

1. Criminal intelligence information of a sensitive nature will be securely stored within the Office of the Deputy Chief of Investigations. The Deputy Chief of Investigations will disseminate internally to affected members of the department information at his/her discretion, upon approval of the Chief of Police.
2. Criminal intelligence information of a non-sensitive nature may be stored by individual units or officers as appropriate. E-mails received from other law enforcement entities labeled "for law enforcement only" may not be shared with non-law enforcement entities or individuals.

E. Dissemination of Protected Information

1. This department's intelligence officer may ONLY disseminate protected information if the following conditions are met:
 - a. The requesting criminal justice agency must certify that it has adopted policies and procedures consistent with this Act. This may be a verbal certification, if the agency is known to the intelligence officer. In the event the agency is unknown, then a signed statement of certification, CHRI Notice of Dissemination form, will be required before release of information.
 - b. The intelligence officer records on the CHRI Dissemination Log the pertinent information for a proper audit trail of disseminated protected information. This record is to be maintained separate from the individual's file.
 - c. The protected information has been determined to be reliable.

- d. The requesting criminal justice agency justifies its request based on name, fingerprints, modus operandi, genetic typing, voice print or other identifying characteristic.
- e. The intelligence officer lists on the CHRI Dissemination Log: the date, purpose and agency requesting information.
- f. In the event the intelligence officer becomes aware of, by any means that previously disseminated information is misleading, obsolete, and/or unreliable, the information is to be collected and the recipient agencies notified of the change within a reasonable time period.
- g. Protected information in the department's possession, but which was not obtained through our sources, may not be disseminated to another agency except if requesting agency and our department are investigating or prosecuting a criminal matter jointly. The intelligence officer must, however, refer the requesting agency to the agency which was the source of the information.
- h. This department's intelligence officer, when requesting protected information from another agency, must certify in writing, CHRI Dissemination Request for Protected Information form that this department complies with CHRIA.

F. Dissemination of Criminal Intelligence Information

- 1. Dissemination of criminal intelligence information must respect the privacy and constitutional rights of individuals, groups and organizations.
- 2. Criminal intelligence information containing personal identifying information (i.e. social security numbers, dates of birth and the like) will not be disseminated outside of the UPPD without the approval of the Deputy Chief of Investigations. Any criminal intelligence information disseminated to other law enforcement agencies containing personal identifying information will be documented; and the documentation shall be retained in the Office of the Deputy Chief of Investigations.
- 3. Criminal intelligence information noted as "law enforcement only" will not be shared with civilian entities.

G. Retention of Records

- 1. The department's protected information and criminal intelligence information will be maintained and will be purged only with the written approval of the Chief of Police and only under the following conditions:
 - a. The data is no longer relevant or necessary to meet the goals and objectives of the UPPD.

- b. The data is obsolete making it unreliable for present purposes and updating it would be worthless.
- c. The data cannot be used for strategic or tactical purposes associated with the duties of the UPPD.

H. Training

- 1. Roll call training on the contents of this directive shall be conducted periodically for both uniformed patrol and members of the Detective Unit.

I. Annual Review of Procedures and Processes

- 1. The Deputy Chief of Investigations, or his/her designee, will conduct a documented annual review of procedures and processes relative to criminal intelligence. This written review will be forward to the Office of the Chief of Police for review and approval.

J. Reporting of Potential Terrorism Related Intelligence/Information

- 1. UPPD officers who observe or obtain terrorist related intelligence or information will document the specifics in writing via memorandum submitted through the chain of command to the Office of the Chief of Police.
- 2. The Chief of Police will review all reports submitted to him regarding potential terrorist intelligence/information or threats to the security of the homeland; and will, based upon the validity of the information, share the facts and circumstances with outside federal, state and local agencies, if warranted.

K. Compliance

Violations of this directive, or portions thereof, may result in disciplinary action.

L. Officers Assigned to Other Agencies

Officers of this department assigned to or assisting other law enforcement agencies will be guided by this directive.

M. Application

This directive constitutes departmental policy, and is not intended to enlarge the employer's or employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims insofar as the employer's or employee's legal duty as imposed by law. Violations of policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.