UW-Madison Police Department

Policy: 82.1
SUBJECT: RECORDS ADMINISTRATION
EFFECTIVE DATE: 06/01/10
REVISED DATE: 05/30/17; 10/17/18; 04/16/19; 10/16/19; 12/04/20
REVIEWED DATE: 04/01/14; 09/04/21
STANDARD: CALEA 82.1.1 – 82.1.6 IACLEA 16.1.7, 16.2.2 WILEAG 10.2.1

INDEX:

POLICY:
The UW-Madison Police Department shall conduct records-related functions in accordance with all applicable state statutes, federal and state regulations, and directives.

DEFINITIONS:
"RMS" system refers to the Department's computerized police record information management system.

PROCEDURE:
82.1.1 PRIVACY AND SECURITY
The following shall establish procedures for securing and controlling access to central records:

A. The privacy and security regulations of the records section are in accordance with the following:
   1. Wisconsin State Statutes 16.61; Records of state offices and other public records
   2. University of Wisconsin Regents policy documents
   3. Wisconsin State Statutes 19.36; Limitations upon access and withholding records
   4. The Freedom of Information Act (FOIA)
   5. The privacy and security of criminal history record information is in accordance with US Department of Justice regulations, Code 28 Part 20, and as governed through Crime Information Bureau TIME System Manual.

B. Central records shall be maintained securely. Privacy and security shall be ensured through adherence to the following precautions:
   1. Disseminating information in accordance with Wisconsin statutes and Federal regulations.
   2. Completing reports in an accurate and timely manner.
   3. Auditing records.
   4. Securing files.
   5. Limiting access.
   6. Reviewing entered data.

C. Access to electronic files shall be restricted to Department personnel. Records are for official use only; under no circumstances shall reports be copied or removed for personal use. Records, supervisory, and investigative personnel, as authorized by the Chief of Police, have access to the locked Records archives.

D. Central records information shall be accessible to operations personnel at all times by physical availability and/or technology.

E. In general, any record generated by the Department is considered an open record. A person or organization that desires a record under this section must file an open records request with the Department. The requestor is responsible for any reasonable cost incurred in reproducing the record. The Department is not required to generate records which do not exist.

F. When making an open records request, Wisconsin statute prohibits asking persons or organizations to identify themselves or state the reason for the request. Requests should be fulfilled as soon as practicable and without delay. Department personnel are not under an obligation to respond immediately to an official open records request.

G. Prior to a defendant having made their initial court appearance, the following information related to the defendant's case may be released:
1. adult defendant's name
2. adult defendant's address
3. adult defendant's occupation
4. arresting officer name
5. the date and time of arrest

H. The department has the authority to withhold or deny open records request based on the balancing test which is inherent in the Wisconsin Public records law.

I. Once the department has identified the records responsive to an open records request, the below conditions shall be taken into consideration prior to responding to a requester in regards to withholding or redacting records:
1. Identifying juvenile information.
2. Sensitive Crimes victim information (such as stalking, harassment, sexual assault.)
3. Information that would identify an informant and anyone who has requested anonymity.
4. Information regarding active and ongoing criminal investigations.
5. Information on police and crime prevention planning, tactics and techniques.
6. Any personally identifiable information that cannot be easily obtained by the average person using other more public means (i.e. social security numbers, dates of birth, driver's license numbers.)
7. Any medical information, whether it is provided as fact or opinion (including the doctor's names, diagnosis, injuries, treatments, medicines, etc.) that is provided by a health care professional.
8. Cases involving active drug, organized crime, gang, and prostitution investigations are confidential and shall not be released without approval from the Chief of Police.
9. Other cases in which the department believes the strong public interest in non-disclosure significantly outweighs the public interest

J. Procedures and responsibilities regarding report and record distribution are delineated in directive 82.2.4.

K. Report processing fees may be charged in accordance with applicable state statutes and policies.

82.1.2 JUVENILE RECORDS

The following shall establish procedures and criteria for the release of Department juvenile records:

A. According to Wisconsin State Statutes 48.396(1) and 938.396(1)(a) a law enforcement agency's records of juveniles shall be kept separate from the records of adults. Thus, all arrests and identification records pertaining to juveniles shall be marked "juvenile" and maintained separately.

B. Juveniles may also be fingerprinted when arrested or taken into custody as deemed appropriate by the arresting officer. However, photographs, fingerprints, and other forms of identifications taken from a juvenile are considered a part of that juvenile's record and subject to the same confidentiality guidelines as other juvenile records.

C. The records supervisor or designee shall be responsible for the collection, dissemination, and retention of Department records pertaining to juveniles.

D. The statutes indicate that the contents of juvenile records may be inspected and their contents disclosed by a law enforcement officer. Officers may have a need for immediate access to juvenile records in the following cases:
1. Conducting child abuse, neglect, and assault investigation.
2. Facilitating taking children into protective custody.
3. Completing referrals to Child Protection for children in need of immediate protection.
4. Completing referrals to Juvenile Intake for criminal and status offenses.

E. Juvenile records are a permanent record and shall remain on file even after the juvenile has become an adult. The juvenile portion of a person's arrest and identification record shall remain restricted, even when the individual reaches

adult age. The disposal of all juvenile records shall be accomplished in accordance with guidelines set by the State of Wisconsin after the individual has reached adult age.

F. Expungement of juvenile arrest records can only be accomplished by a valid court order.

82.1.3 RECORDS RETENTION SCHEDULE

A. The Department shall establish, maintain and follow a record retention schedule. Adherence to such a schedule shall ensure that electronic data and written documentation is stored and purged in an orderly manner.

B. The Support Services Captain or designee shall be responsible for the following:
   1. Determining retention needs
   2. Purging stored information is a secured manner
   3. Converting data
   4. Updating schedules

C. The Support Services Captain or designee shall ensure compliance with legal and administrative requirements.

82.1.4 UNIFORM CRIME REPORTING SYSTEM

A. The Department shall participate in approved state and national crime reporting programs. Such participation assists in effective internal records maintenance and aids in the effort to establish a national database of crime/incident statistics.

B. Department crime data shall be collected via complete incident reports and other resources outlined in department directive 15.1 Crime Analysis. Such information shall be entered into electronic systems in a timely manner.

C. Records Staff collects statistical crime data for the FBI required Monthly Report. Monthly reports shall be prepared by Records Staff and reviewed by the Investigative Captain or designee. These reports shall be sent to the Wisconsin Department of Justice.

82.1.5 REPORT STATUS PROCEDURE

A. All calls for service shall be identified through sequential event (control) Computer Aided Dispatch (CAD) generated numbers. In addition to the above listed event ID, an incident report number shall be assigned for cases involving:
   1. A criminal event
   2. All arrests
   3. Felony, misdemeanor, or non-traffic forfeiture offenses
   4. Death investigations
   5. Potential University liability, such as significant injury caused while on the UW-Madison campus, potential release of biological agents, etc.
   6. Incidents as directed by a supervisor,
   7. Incidents that, by their nature, require investigation and documentation.

B. A Field Contact entry shall be done to document contact with identified citizens for incidents which do not meet the criteria for an incident report.

C. Coded disposition entries within CAD shall be utilized to record complaint status. For all events requiring a report, the incident status shall be included with the report number. Records unit personnel shall compare incident status entries and CAD information to ensure the accuracy and accountability of control numbers. Affected personnel shall be notified of any discrepancies as soon as possible.

D. Communication center personnel shall maintain a list of CAD generated numbers that have not been disposed of on the daily briefing sheet. The supervisor of the employee responsible for the completion of the disposition shall ensure that it is completed in a timely fashion.

E. Records Staff shall account for the status of initial reports. This tracking may be done through established mechanisms in the RMS database or other reliable means.

F. If a report requires a follow-up investigation by the reporting officer, the officer shall attempt to complete the investigation in a timely fashion. The status of follow-up investigation or reports shall be tracked by the field supervisor. This tracking may be done through electronic mechanisms or other reliable measures.

G. All supplemental reports shall contain the same incident report number as the original investigation and shall receive the same review process as the preliminary case report. The supervisor of the employee responsible for the completion of a supplementary report shall ensure that it is completed in a timely manner.

H. The Investigative Services Captain or designee is responsible for assigning cases and for investigative case control.

I. Incident reports and supplements shall utilize a classification system to indicate current case status. Such classifications include: active, inactive, cleared by arrest, unfounded, exceptional clearance, other, and closed.

82.1.6 COMPUTER FILE BACK-UP AND STORAGE

The following describes the process for maintaining security of central records computer systems:

A. Computer files that reside on the Local Area Network (LAN) and the records database server are backed up on a daily basis. Such backups shall be conducted in accordance with applicable state statutes, record retention schedules, and directives. All backup computer files are secured and stored off-site. Access to the secure backup computer files is limited to the Support Services Captain and IT staff. Tapes used to backup computer files are recycled until such time as they become unusable. Methods of destruction shall ensure that data is not retrievable from discarded materials.

B. Computer hardware containing the Local Area Network (LAN) and the records database server are housed within secure server rooms in the Department. Media, tapes, disks, drives or other types of electronic media containing sensitive, confidential or restricted records that are stored or travel outside of the physically secured offices of the Department shall be encrypted. Server and workstation hard drives and other media used for central records storage shall either be reused or shall be physically destroyed.

C. Physical access to the server rooms housing the central records servers shall be limited to supervisory and IT personnel. Physical access to workstations connected to the Department network shall be limited to current employees. Electronic access to central records is limited to current Department employees who have passed background checks. Password age and strength levels shall be set and maintained by the server operating system and UW-System Policies. Electronic communication or transfer of sensitive, confidential or restricted data outside of the department network shall be encrypted.

D. The department maintains an automated system for verification of passwords, access codes, or access violations. The IT Manager or designee is responsible for administering the automated system and security of records contained therein.

82.1.7 COMPUTERIZED CRIMINAL HISTORIES

The following shall establish a security protocol for access to and release of criminal history records:

A. The dissemination of computerized criminal history information must conform to the rules and regulations outlined in the Crime Information Bureau Transaction Information for the Management of Enforcement (TIME) User's Manual.

B. Criminal history information must be afforded strict privacy considerations. Access to criminal history records shall be limited to sworn officers, dispatchers, and Court Services and Records Personnel. When requesting record checks using the TIME System, personnel must use the TIME System approved criminal query format. The reason the information is requested must be submitted by utilizing the appropriate purpose code, Event/Report Number, and/or name of the person requesting the data.

C. NCIC policy prohibits the routine dissemination of criminal history information by radio or wireless telephone. Such dissemination is possible when an officer or LED determines there is an immediate need for the information to further an investigation or in situations affecting the safety of an officer or the general public.