



Republic of the Philippines
NATIONAL POLICE COMMISSION
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
OFFICE OF THE CHIEF, PNP
Camp BGen Rafael T Crame, Quezon City

MAY 20 2020

MEMORANDUM CIRCULAR

NO.: 2020-037

POLICE BLOTTER AND CIRAS INFORMATION ACCESS

1. REFERENCES:

- a. The 1987 Philippine Constitution - Section 7, Article III which reads as "The right of the people to information on matters of public concern." b) Section 28, Article II which states that "The State adopts the policy of full public disclosure of all its transactions involving public interest.";
- b. Republic Act No. 11032 "Ease of Doing Business and Efficient Government Service Delivery Act of 2018";
- c. Republic Act No. 10173 "Data Privacy Act of 2012";
- d. Republic Act No. 9344 "Juvenile Justice and Welfare Act of 2006";
- e. Republic Act No. 9262 "Anti-Violence Against Women and Their Children Act of 2004";
- f. Republic Act No. 7610 "Special Protection of Children Against Abuse, Exploitation and Discrimination Act";
- g. Executive Order No. 02, series of 2016 dated July 23, 2016 titled "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor."
- h. Memorandum from the Executive Secretary, Office of the President of the Philippines, dated November 24, 2016 with the subject "Inventory of Exceptions to Executive Order No. 2, series of 2016.";
- i. PNP Freedom of Information (FOI) Manual published 2018; and
- j. Standard Operating Procedure No. 2012-001 dated March 26, 2012 "Incident Recording System (Procedure in Recording Incident Reports in the Police Blotter)."

2. RATIONALE:

The Philippine National Police (PNP), as the country's premier police agency, is organized for the purpose of facilitating the attainment of its goals and objectives which calls for a streamlined and airtight investigation service that is responsive to the rights, needs and demands of stakeholders.

As the Directorate primarily responsible in overseeing and safekeeping of all crime information, the Directorate for Investigation and Detective Management (DIDM) emphasizes its commitment in upholding the fundamental right to privacy and communication while ensuring free flow of information to promote innovation and growth. It further recognizes the role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in

**CERTIFIED TRUE COPY
FROM ORIGINAL**

Page 1 of 10


JOD L. DELA ROSA
Police Lieutenant Colonel
Administrative Officer

information and communications system within the Directorate's custody are secured and protected.

To abide to the organization's commitment, a policy should be instituted to ensure the security of all investigation records and its safekeeping from potential information leakage tantamount to violation to the right of privacy of the real party-interest.

3. SITUATION:

Since 2016, the DIDM has been utilizing the Crime Information, Reporting and Analysis System (CIRAS) as the repository of all crime incident information emanating from the complaints received by police stations and those written in police blotter. Such reports include personal information of complainants, victims, and suspects; and other vital information as to how incidents transpired, including those that may affect the welfare of the victims and suspects, which are deemed confidential. Moreover, police blotter entries bear details imperative to the advancement of cases filed in court. Thus, disclosure of the same to anyone, most specially to those who are not directly involved, may result to information misuse which in effect may further jeopardize the advancement of the case.

Because the police blotter is considered a public document, stakeholders such as media practitioners and students among others have perceived such as a document which they can freely access, view, browse, and reproduce. However, the study conducted by the DIDM revealed that such practice violates existing laws and policies such as the Data Privacy Act of 2012 and the provisions stated in the PNP FOI Manual.

The Data Privacy Act of 2012 prohibits the disclosure of any personal information without the consent of the data subject of the information. For example, a blotter entry which indicates the name, age, and address of a suspect shall not be divulged to anyone without the permission of the person concerned.

In consonance, under the provisions stipulated in the PNP FOI Manual, the PNP shall ensure that information in its custody or under its control is disclosed only as permitted by existing laws and shall likewise protect personal information in its custody or under its control by making reasonable security arrangements against unauthorized access, leaks or premature disclosure.

While the police blotter is considered a public document, it is bound to be treated as confidential under Rules of Court, Data Privacy Act of 2012 and other policies, especially information that pertains to a case or facts relative to the commission of crime. The right of the accused to be presumed innocent would be violated if such document or information would be easily obtained by non-real party interest, such as the media where the control to its dissemination could no longer be done if already released.

Thus, in order to provide tailor-fitted guidelines in accordance with existing laws and policies to protect the right to privacy of real party interest and to avoid information leakage that may affect the progress of ongoing cases, a policy shall be created to

**CERTIFIED TRUE COPY
FROM ORIGINAL**

Page 2 of 10


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer

Police Lieutenant Colonel
Administrative Officer

streamline the process of information access of those written in police blotter and those reflected in the CIRAS database.

4. PURPOSE:

This Memorandum Circular sets forth the guidelines and procedures in the proper management and information access of data written in the police blotter and those encoded in CIRAS.

5. DEFINITION OF TERMS:

- a. Crime Information, Reporting and Analysis System (CIRAS) – formerly the e-Blotter system that sets a standard procedure by which all crime incidents reported to the police stations are electronically stored in a database. The system does not only facilitate crime documentation and storage but also presents a quick, fast, and reliable transmission of crime information from a particular police station to the National Headquarters at Camp BGen Rafael T Crame, Quezon City.
- b. CIRAS Entries – are details collected from the complainants or victims regarding the incidents submitted for recording. These records contain sensitive and personal data such as name, address, age, of concerned persons.
- c. Data Subject – refers to an individual whose personal information are processed.
- d. Internal Stakeholders – persons/units/offices within the PNP that are affected by the implementation of this MC.
- e. External Stakeholders – persons/units/offices outside the PNP that may be affected by the implementation of this MC. These include students, members of the academe, other law enforcement agencies, media practitioners and the likes.
- f. Information Access – the ability of a person to view or acquire a specific information.
- g. Police Blotter – an official logbook, covered blue with hardbound cover that contains the daily register of all crime incident reports, official summary of arrests and other significant events/activities reported in the police station. Relatedly, a separate pink blotter for WCPD to record all cases involving violence against women and children and those cases involving a child in conflict with the law that fall under the mandate of WCPDs.
- h. Real Party-Interest – a party who stands to be benefitted or injured by the judgement in the suit or the party entitled to the avails of the suit.
- i. Requesting Party – A person/organization, who is not a data subject, who applies for an access or copy of an information.

**CERTIFIED TRUE COPY
FROM ORIGINAL**

Page 3 of 10


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer

- j. Record Reproduction – the act of reproducing records in the form of photocopying, photo-capturing, re-transcribing and the like.
- k. Information leakage – the act of transmitting, divulging, or reproducing records through any form without consent from the Information Owner or order from the courts.
- l. Higher Authorities – any PNP official holding a position of head of office of a higher unit (e.g. Regional Director).
- m. PNP Personnel – any personnel working in the PNP who holds a regular position and has any corresponding restriction access. It may be Uniformed or Non-Uniformed Personnel.
- n. Unauthorized Personnel – Any personnel who does not hold any clearance or authority to view and reproduce records. Likewise, these personnel are also those who do not hold any authority to approve any requests for information access.
- o. WCPC e-Blotter – a part of CIRAS which stores data related to all WCPC blotters, and may only be accessed by PNP personnel directly involved in their respective cases involving women and children.

6. GUIDELINES:

a. General Guidelines:

- 1) The police blotter and CIRAS entries are considered properties of the PNP and its officers shall be held responsible for its confidentiality;
- 2) Police blotter and CIRAS entries contain personal information of complainants, victims, and suspects. Under the Data Privacy Act of 2012, the same shall not be divulged to anyone unless they are among the real party-interest or there is an order from the court;
- 3) Access to the police blotter and CIRAS shall be only be limited to PNP personnel. All PNP personnel who have accessed the information from the police blotter, Pink Blotter, and CIRAS shall maintain the confidentiality of all information therein and ensure that such are free from information leakage;
- 4) All information requests shall be denied except those issued by the data subject or information owner, or those issued by the courts;
- 5) As provided by Republic Act No. 9262, information from the Pink Blotter shall not be divulged to anyone except those who are directly involved in the investigation of the case;

- 6) As provided by Republic Act No. 6713, sec 7, paragraph (c), Public officials and employees shall not use or divulge, confidential or classified information officially known to them by reason of their office and not

made available to the public either to further their private interests, or give undue advantage to anyone; or to prejudice the public interest; and

- 7) All information requests from real party-interest shall observe the process under the PNP FOI Manual.

b. Specific Guidelines

1) Maintaining and Confidentiality of WCPC Records:

- a) All police officers who are working on a WCPC case shall ensure a faithful recording of all pertinent information involving women and children;
- b) Only WCPD personnel shall have access to the Pink Blotter and the WCPC e-Blotter;
- c) As provided in Section 43 of Juvenile Justice and Welfare Act as amended, the records of a CICL shall not be used in subsequent proceedings, whether criminal, civil, or administrative, for cases involving the same offender as an adult, except when beneficial to the offender and upon the offender's written consent;
- d) Collective information and statistics generated from the WCPC e-Blotter shall only be used for research, policy, program development, monitoring and evaluation purposes;
- e) All records of the CICL in the custody of the WCPD and other units shall be sealed by order of the court. The case shall be treated as if it never occurred. All index references shall be deleted and in case of injury, all police officers shall reply that no record exist with respect to the child concerned;
- f) All unit commanders shall ensure the exclusion of public and other uniformed personnel not directly involved in the WCPD case from accessing information therein;
- g) The disclosure of confidential records may only be done upon Order of the Court. The records of the CICL may only be disclosed to persons specifically enumerated in the Order of the Court permitting such disclosure, and subject to such conditions as the Court may impose; and
- h) When applicable, advise the media to observe the Guidelines for Media Practitioners on the Reporting and Coverage of Cases Involving Children under the Department of Justice.

2) Information Access and Management:

- a) All PNP Personnel shall only be allowed to view police blotter and CIRAS entries for official purposes or for the purpose of carrying out their duties. Divulging of information therein shall not be allowed

Page 5 of 10

CERTIFIED TRUE COPY
FROM ORIGINAL


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer

without consent from the data subject or without an order from the Courts;

- b) No form of reproduction (e.g. photocopying, reprinting, or photo capturing) of the Incident Record Form (IRF) or other information shall be performed without the approval of the head of office, provided that the copies will only be used for official purposes, provided further that the requesting party is among those who are permitted under existing laws to request for a copy;
 - c) Data subjects or his/her next of kin, if the former is in anyway incapacitated, may be allowed to have access on police blotter information. Next of kin may request for a copy of the information provided that a formal request is issued in accordance with the procedure set forth by the PNP FOI Manual;
 - d) Data requests from external stakeholders such as media, students, researchers, etc. shall, at all times, be coursed through the Public Information Officer of the Station or, in case of higher offices, through their respective Public Information Office; and
 - e) Police stations can release crime statistics to external stakeholders provided that said parties submitted a formal request stating the exact information they needed and for what purpose said information will be used. The said request shall then be submitted to the head of office for its approval.
- 3) Application, Activation, and Deletion of CIRAS access:
- a) The Chief of Police of the requesting station shall issue an endorsement memorandum addressed to their immediate Police Provincial Office or District Office for the activation of CIRAS accounts of their respective personnel. The same process shall be applied for the deletion of inactive accounts, should registered encoders are reassigned or designated to other positions;
 - b) The Police Provincial Office shall endorse the said requests to their respective Police Regional Office for subsequent endorsement to DIDM; and
 - c) The DIDM shall apply necessary actions to the request based on the endorsement memorandum received from PROs.
- 4) Guidelines for CIRAS generated data and statistics:
- a) All personnel shall only provide a copy of the IRF to the data owner and shall likewise refrain from giving out copies to other persons or entities except when required by the courts;
 - b) All crime statistics generated from CIRAS shall indicate the time and date of extraction, and a watermark stating "UNLAWFUL USE OR

**CERTIFIED TRUE COPY
FROM ORIGINAL**


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer


ALTERING OF DATA IS PUNISHABLE BY LAW" shall be placed diagonally in the document;

- c) The name and signature of the PNP personnel who extracted and processed the data shall be indicated at the lower left section of the document with "Prepared by:" written above it;
 - d) The name and signature of the PNP personnel who verified the data shall be indicated at the lower middle section of the document with "Verified by:" written above it;
 - e) The name and signature of the head of office/unit/section shall be indicated in the lower right section of the document with "Noted by:" written above it; and
 - f) All statistics generated through CIRAS shall be coursed through proper channel and shall observe the process under the PNP FOI Manual.
- 5) Request for Information:
- a) The requesting party should:
 - (1) Observe the process of availing of information under Chapter 2.1 of the PNP FOI Manual;
 - (2) Indicate in the request a brief description of the information being requested, and the reason and purpose for requesting such information. Absence of required information may be a ground for the denial of the request;
 - (3) Identify himself by presenting two valid IDs upon submission of the request for information. Failure to properly identify himself/herself may be a ground for the denial of the request; and
 - (4) State his/her desired mode of receiving the requested information (i.e. electronic mail, postal mail).

As provided Chapter 2.6 of PNP FOI Manual, the requested information may be received through the following means:

- (a) The requesting person can personally receive the requested information at the FOI Office where he submitted his/her request;
- (b) The information may be released in electronic file, in which the requesting person shall provide material or gadget necessary for copying the files free of charge; and
- (c) In case the information requested cannot be processed within the day, or if the requesting person wishes to receive it via postal mail or private courier, he/she shall be asked to

**CERTIFIED TRUE COPY
FROM ORIGINAL**


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer

coordinate with the nearest PNP office/unit to which the requested information will be transmitted;

- b) If the requesting person is asking for public information on behalf of someone else, he/she must submit an authorization letter from the information owner or Special Power of Attorney;
- c) It shall be the responsibility of the FOI Decision Maker to determine the disposition of the data requested according to the PNP FOI Manual.
 - (1) If the request is granted, the document or data requested shall be provided within 15 working days; or
 - (2) If the request is denied then the receiving office shall inform the requestee of the reason why the request was denied within 15 working days.

7. Responsibilities


- a. Directorate for Investigation and Detective Management (DIDM)
 - 1) Responsible for the strict implementation of this MC down to the lowest PNP unit;
 - 2) Coordinate with PIO regarding the proper implementation of this MC;
 - 3) Ensure that the guidelines set forth by this MC are properly followed and applied by all PNP units, particularly those with investigation function, those which maintain police blotter, and those which have access in CIRAS; and
 - 4) Perform other tasks as directed.
- b. Directorate for Police Community Relations (DPCR)
 - 1) Assist DIDM in the proper implementation of this MC;
 - 2) Disseminate this policy guidelines to stakeholders;
 - 3) Establish rapport with stakeholders for their cooperation in the implementation of this MC; and
 - 4) Perform other tasks as directed.
- c. Public Information Office (PIO)
 - 1) Assist DIDM in the proper implementation of this MC;
 - 2) Ensure that all public information units and personnel of the PNP are well-informed and will execute this MC;
 - 3) Maintain lateral and vertical coordination with all units in the implementation of this MC; and

**CERTIFIED TRUE COPY
FROM ORIGINAL**


JOE B. L. P. 224
Police Lieutenant Colonel
Administrative Officer

- 4) Perform other tasks as directed.
- d. Police Regional Offices (PROs)
 - 1) Ensure the proper dissemination and application of this MC to all lower units;
 - 2) Coordinate with Regional PIO for proper implementation of this MC within respective office;
 - 3) Monitor compliance of lower units; and
 - 4) Perform other tasks as directed.
- e. Police Provincial Offices (PPOs)/District Offices/City Police Offices (CPOs)
 - 1) Ensure the proper dissemination and application of this MC to all lower units;
 - 2) Coordinate with Provincial/District/City PIO for proper implementation of this MC within respective office;
 - 3) Monitor compliance of lower units; and
 - 4) Perform other tasks as directed.
- f. Chief of Police/Station Commanders
 - 1) Supervise, monitor and ensure the proper application of the guidelines set forth by this MC;
 - 2) Act as the Approving Authority for your respective unit;
 - 3) Maintain a journal of all requests received by your respective unit and corresponding actions taken. Entries shall bear the date received, actions taken, and date of response;
 - 4) Designate a police officer who will act as the Public Information Officer; and
 - 5) Perform other tasks as directed.
- g. Station-level Public Information Officer
 - 1) Act as the FOI Decision Maker;
 - 2) Filter all requests and decide whether such request may be granted or not. Refer to the PNP FOI Manual, this MC and other related policies as guide for decision-making;
 - 3) Submit proposed disposition to the approving authority for approval; and
 - 4) Perform other tasks as directed.

**CERTIFIED TRUE COPY
FROM ORIGINAL**


JOB L. DE MESA
Police Lieutenant Colonel
Administrative Officer

8. PENAL CLAUSE:

Any violation of this MC shall be dealt with accordingly pursuant to existing laws, rules and regulations. All Unit Commanders shall be included in the investigation under the principle of Command Responsibility.

9. REPEALING CLAUSE:

Any provision of issuances, memoranda, rules and regulations issued by the PNP inconsistent herewith are deemed repealed or amended accordingly.

10. EFFECTIVITY:

This MC shall take effect after 15 days from filing a copy thereof at the UP Law Center in consonance with Section 3, Chapter 2, Book VII of Executive Order 292 otherwise known as the "Revised Administrative Code of 1987," as amended.




ARCHIE FRANCISCO F GAMBOA
Police General
Chief, PNP

Distribution:
Command Group
D-Staff
P-Staff
RDs, PROs
D, NSUs
IG, IAS

Copy Furnished:
SPA to SILG

CPNP Ltrs'20 S081744



S081744

**CERTIFIED TRUE COPY
FROM ORIGINAL**


JOB L DE MESA
Police Lieutenant Colonel
Administrative Officer