PROCEDURE MANUAL
14-02

MICHIGAN STATE POLICE

Privacy of Personally Identifying Information

Purpose: This manual provides guidance and procedures to ensure the privacy of Potentially Personally Identifiable Data (PPID) that may be used, collected, or retained by the Michigan State Police (MSP).

Effective Date: July 05, 2022

Table of Contents

Definitions:

Potentially Personally Identifiable Data (PPID): Is a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, taxpayer identification number, health insurance identification number, credit card number, IP Address, or medical information. Some data elements alone may not be considered personally identifiable, but when combined with other information can be linked to a person. For example, date of birth, ethnic background, gender, height, and weight can be considered potentially identifiable information when combined with other data elements. PPID is comprised of more data elements than those listed above; you should check the federal and state laws applicable to the data potentially in your care using terms such as PHI, PII, FTI, PPI, CJI, PCII, and Student Education Records from FERPA.

Section 1:

1.1 Data Privacy

a. These policies and procedures are applicable to all PPID held or used by the department, regardless of the format (electronic, printed, etc.), the technology used to handle or store it, or the purposes it serves.

b. The department has selected and adopted the American Institute of Certified Public Accountants' Generally Accepted Privacy Principles (GAPP) as our privacy framework. The intent of this section is to implement this framework, as required by Policy 2610.01, and to ensure that

every precaution is taken to protect the privacy of those who entrust the department with their personal information.

1.2 Compliance with Administrative Guide to State Government, Policy Group 2600 – Privacy

a. By reference, the department implements and will comply with all standards, policies, and procedures contained within Policy Group 2610, Privacy of the State of Michigan's Administrative Guide to State Government (Ad Guide).

1.3 Privacy Notice

a. The department shall develop and maintain a public privacy notice in compliance with procedure 2610.02, privacy notice. The privacy notice shall be posted on the department's website.

b. The Privacy Protection Officer shall be responsible for maintaining the privacy notice and has been identified by the Director as the point-of-contact for questions regarding privacy of department information.

c. Any member who maintains potentially personally identifiable data (in any format) in a manner that differs from the information provided in the privacy notice shall immediately notify the Privacy Protection Officer.

d. The Privacy Protection Officer shall maintain a list of individuals who have submitted (in writing) a request to be notified of changes to the privacy notice. The Privacy Protection Officer shall send notification to those individuals any time changes are made to the privacy notice.

e. The Privacy Protection Officer shall ensure that the privacy notice is reviewed annually and updated whenever necessary.

f. The Privacy Protection Officer shall electronically distribute the privacy notice to all members any time changes are made to the notice. The distribution shall include an explanation of the changes made since the last revision.

g. The Privacy Protection Officer shall maintain documentation of changes made by each iteration of the privacy notice, privacy policy, and privacy procedure.

1.4 Choice and Consent

a. Members shall not disclose, make available, or use an individual's PPID for purposes other than those specified in the privacy notice, except with written consent of the individual, or as authorized by law.

b. The privacy notice shall describe any situations where an individual has a choice to consent in allowing the department to collect, use, or disclose their information.

   i. Consent and accommodations are not generally required to process PPID where applicable laws impose obligations on the department to process it.

   ii. In situations where an individual has the choice to consent, the privacy notice must identify how an individual can revoke their consent at a future date.

c. The PPID may only be obtained by lawful and fair means, and where appropriate or required by law.

d. Individuals with concerns regarding the collection, use, or disclosure of their PPID within a specific worksite or information system shall be directed to contact the commander responsible for that worksite or information system. Otherwise, the individual shall be directed to contact the Privacy Protection Officer.

1.5 Individual Access

a. Where an individual has the right of access to the PPID maintained by the department, the department must provide individuals, upon request, with a reasonable opportunity to review, and possibly correct, their PPID.

b. Any method that an individual may use to directly request, access, review, or correct PPID in possession of the department shall be published in the privacy notice.

c. All written requests submitted to any member by an individual requesting access to their own personal information shall be treated as a "Freedom of Information Act" request and forwarded to the Records Resource Section for appropriate action, per the written directive related to Freedom of Information Act.

d. All other requests for access to information shall be directed to contact the Records Resource Section.

e. Individuals with concerns regarding the accuracy or privacy of PPID held within a specific worksite or information system shall be directed to submit a written request to the commander responsible for that worksite or information system. Otherwise, the individuals shall be directed to submit a written request to the Privacy Protection Officer. The written request must provide a descriptive explanation of the issue and include supporting documentation.

    i. If the department denies an individual's request to correct or amend a record, and there is not a specific procedure or remedy that exists under state or federal law or collective bargaining agreement, the individual may submit a written appeal to either the Privacy Protection Officer or the Director.

    ii. If the requested change is required by law or if otherwise reasonably possible, however no correction is made in response to the written request by an individual to correct or amend disputed PPID, the member processing the request must annotate in the record that a correction or amendment was requested but not made and include a copy of the request and a reason why the correction was not made.

    iii. If the requested change requires the use of a court procedure, the individual must be informed of this.

f. Members must be mindful of protecting the individual's PPID throughout this process. Members must first authenticate the individual requesting information is the individual associated to the source record prior to providing any information or initiating any changes.

    i. Members must receive annual training on authenticating the identity of an individual before they will be authorized to either disclose or amend a record containing an individual's PPID.

ii. Individuals requesting access or changes to PPID must be able to produce government issued identification that confirms the identity of the requestor prior to release of any personal information associated to the requestor. Biometric verification of identity may be used in circumstances where identification cannot be produced.

iii. If mailing PPID to an individual, only mail that information to the current address of record. In the case of an address change, a notice of the request or change shall be sent to both the old address and the new address.

1.6 Management and Accountability

a. The Privacy Protection Officer determines which laws are applicable to their PPID and monitors state and federal privacy laws, regulations, and policies for changes that may affect department programs. The Privacy Protection Officer, with legal counsel, will review compliance with privacy policies, practices, controls, and procedures annually.

1.7 Security for Privacy

a. All members with access to PPID must annually complete the State of Michigan Security and Privacy Awareness Training, to ensure members understand privacy responsibilities and procedures.

b. All members with access to data classified as agency sensitive, classified, or restricted must complete the MSP Security Awareness Training every two years, to ensure members understand internal IT security requirements and procedures.

1.8 Collection

a. PPID may only be collected for the purposes identified in the privacy notice.

b. PPID may only be collected to the extent it is required for the purpose that it is collected, unless otherwise required by law or rule.

c. A commander overseeing a worksite or information system which retains PPID shall annually review the purpose and need for collecting the PPID, to determine if there are any data fields that are no longer necessary and to adjust the collection of PPID accordingly.

d. Before a worksite or information system begins to collect and retain new or additional PPID information, the commander overseeing the worksite or information system shall consult with the Privacy Protection Officer to ensure that the collection of information is in alignment with the privacy notice, that the data is obtained fairly (without intimidation or deception) and lawfully.

e. Third-Party PPID Data Collection

i. PPID information obtained from a third-party data provider may only be used and retained if it is from a reliable source and the information is obtained fairly and lawfully. The Privacy Protection Officer is the person within the department responsible for making this determination.

ii. The Privacy Protection Officer shall update the privacy notice to reflect the use of third-party data providers prior to use. The privacy notice shall identify the third-party data provider by name, list the PPID information obtained from that provider, and specify how that information is being used.

1.9 Use, Retention, and Disposal

a. PPID may only be used for the purposes identified in the privacy notice, or as required by law, regulation, or rule.

b. PPID may not be retained longer than necessary to fulfill the purpose that it was collected for, unless otherwise required to be retained by law, regulation, or rule.

c. Retention and disposal of PPID data must comply with the policies listed in the privacy notice related to the purpose that the PPID was collected. If policies are not specifically identified, Federal Bureau of Investigation, Criminal Justice Information System (CJIS), Security Policy standards for retention and disposal of CJIS must be met.

d. Retention and disposal of all department data must comply with written directive related to disposition of records. The department and State of Michigan Retention Policies can be found on the Intranet.

1.10 Disclosure to Third Parties

a. PPID may only be disclosed to a third-party for a purpose listed in the privacy notice at time of PPID collection unless the disclosure is specifically authorized by law or if written consent is obtained from the individual prior to disclosure.

b. All agreements to share information with a third-party must be reviewed and approved by the Privacy Protection Officer, and the agreement must include:

   i. Controls that assure PPID is protected in a manner that is consistent with the protections required for the department.

   ii. Ability to audit the third-party for compliance with privacy controls, policies, and practices, at the discretion of the Privacy Protection Officer.

   iii. Limitations that ensure PPID can only be used for the purpose required to fulfil the contract.

   iv. Security and Privacy Awareness Training for individuals with access to PPID.

   v. Penalties for misuse of PPID.

   vi. Direct point-of-contact for individual responsible for addressing security and privacy concerns related to the PPID.

1.11 Quality

a. The commander responsible for the worksite or information system collecting PPID shall ensure that any PPID retained or used by the department is complete and accurate.

b. Retention and use of PPID must be relevant to the purpose that it was collected.

c. The date that PPID is both obtained and last updated shall be recorded.

d. The source of the PPID shall be recorded, whenever possible.

e. Periodic assessments shall be conducted to verify the accuracy of the record and to ensure that it is being used for the purpose that it was collected.

1.12 Monitoring and Enforcement

a. Inquiries, Complaints, and Disputes regarding privacy policies and procedures shall be directed to the Privacy Protection Officer.

b. The Privacy Protection Officer shall document and respond to all complaints within five business days. Complaints that cannot be resolved by the Privacy Protection Officer will be escalated to the appropriate work unit commander, or the Director.

c. The Privacy Protection Officer shall conduct an annual review of privacy policies and procedures to ensure continued compliance with Policy Group 2610-Privacy, in the State of Michigan Administrative Guide to State Government.

d. Any violation of this policy shall be treated as a security incident. The Information Security Officer, the CJIS Security Officer, and the Privacy Protection Officer shall be immediately notified of the violation. The reporting party shall complete a security incident report, CJIS-016, as soon as reasonably possible to document the incident.

e. The Information Security Officer and the Privacy Protection Officer will annually review privacy incidents, complaints, internal control evaluations, and available audit reports to evaluate compliance and recommend policy or procedural changes.