Department of the Prosecuting Attorney

Maui County

Privacy Policy

John D. Kim
Prosecuting Attorney
October 2014

Department of the Prosecuting Attorney

County of Maui

Privacy Policy

October 2014

Date Submitted:
October 31, 2014

Approved By:

John D. Kim,
Prosecuting Attorney
County of Maui

Purpose

As directed by the HIJIS Privacy Policy, in order for participating agencies to participate in the HIJIS framework, they must have an existing privacy policy. This privacy policy adopts the template that was developed by the Global Justice Information Sharing Initiative (Global). The Department of the Prosecuting Attorney for the County of Maui has chosen to use this template to develop its privacy policy.

Policy Applicability and Legal Compliance

1. All Department of the Prosecuting Attorney, Maui County (**DPAMC**) personnel, personnel providing information technology services to the agency, private contractors, entities from which agency information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to refer to the listing in the HIJIS privacy policy, Appendix A, and the Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information, Appendix B.

2. The **DPAMC** has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to:
   HRS Chapter 92F (Uniform Information Practices Act),
   HRS §§ 286-171 and 286-172 (Traffic Records),
   HRS Chapter 291C (statewide Traffic Code),
   HRS Chapter 353 (Corrections),
   HRS Chapter 487J (Social Security Number Protection),
   HRS Chapter 487N (Security Breach of Personal Information),
   HRS Chapter 571 (Family Courts),
   HRS Chapter 846 (Hawaii Criminal Justice Data Center),
   HRS Chapter 846D (Juvenile Justice Information System),
   Federal Code 28USC §534 (FBI Identification Records and Information),
   Hawaii Rules of Penal Procedure,
   Hawaii Rules of Civil Procedure,
   Hawaii Court Records Rules,
   Hawaii Electronic Filing and Service Rules, and
   Hawaii Rules of Professional Conduct.

Governance and Oversight

1. Primary responsibility for the operation of the **DPAMC**; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of the HIJIS Privacy Policy, as well as the **DPAMC** Privacy Policy, is the Prosecuting Attorney of the County of Maui.

Information

1. The DPAMC will seek, retain, and share information through the HIJIS framework that:
   - Is based on a possible threat to public safety or the enforcement of the criminal law, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is relevant to an investigation and prosecution of a suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

2. The **DPAMC** will not seek or retain information that will be shared through HIJIS and information-originating entities will agree not to submit information through HIJIS about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. The **DPAMC** applies labels to agency-originated information (or ensures that the originating agency has applied labels) that will be shared through HIJIS to indicate to the HIJIS-accessing authorized user that:
   - The information is "protected information," to include a "personal record" on any individual (see Definitions, within the HIJIS policy) and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to local, state, or federal laws restricting access, use, or disclosure.

4. The **DPAMC** personnel will, upon receipt of information that is intended to be shared through HIJIS, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).

- The information should be viewed as reliable and valid unless otherwise noted (for example, information that is not positive ID based).

5. At the time a decision is made by the **DPAMC** to retain information that is intended to be shared through HIJIS, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Protect an individual's right of privacy.
   - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information that is shared through HIJIS will be reevaluated whenever:
   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. The **DPAMC** requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content), that will be shared through HIJIS, for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information may include all or some of the following:
   - The name of the originating agency, department or agency, component, and subcomponent.
   - The name of the agency's justice information system from which the information is disseminated.
   - The date the information was collected and, when feasible, the date its accuracy was last verified.
   - The title and contact information for the person to whom questions regarding the information should be directed.

8. The **DPAMC** will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated through HIJIS to clearly indicate any legal restrictions on intra-agency information sharing, within the agency accessing the information, based on information sensitivity or classification.

Acquiring and Receiving Information

1. The information-gathering (acquisition), access, and investigative techniques used by the **DPAMC** and information-originating entities will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information, where applicable.
- The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or agency policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP), where applicable.
- Constitutional provisions; statute, the Policy Applicability and Legal Compliance section in this document; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

2. The information-gathering and investigative techniques used by the **DPAMC** and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information the agency is authorized to seek or retain.

3. The **DPAMC**, in accessing information through the HIJIS framework or sharing information through HIJIS assures that it will comply with laws and rules governing the entity, including applicable federal and state laws.

4. The **DPAMC** will contract only with contractors and vendors that provide an assurance that their methods for gathering information—information that will, ultimately, be shared through HIJIS—comply with applicable local, state, tribal, territorial, and federal law and that these methods are not based on misleading information-gathering practices.

5. The **DPAMC** will not directly or indirectly receive, seek, accept, or retain information that is intended to be shared through HIJIS from:
   - An individual who or nongovernmental agency that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or agency policy.
   - An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

Information Quality Assurance

1. At the time of retention in the **DPAMC** system, information that will be shared through HIJIS will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

2. The labeling of retained information that is shared through HIJIS will be reevaluated by the **DPAMC** or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

3. The **DPAMC** should conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted, or not used when the agency identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the agency did not have authority to gather the information or to provide the information to another agency; or the agency used prohibited means to gather the information (except when the agency's information source did not act as the agent of the agency in gathering the information).

4. Participating agencies, such as the **DPAMC**, are responsible for reviewing the quality and accuracy of the data provided through HIJIS. The **DPAMC** will review the quality of information, that it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

Collation and Analysis

1. Information acquired, received, or accessed by the **DPAMC** through HIJIS will be analyzed only by authorized individuals who have been trained accordingly.

2. Information accessed through the HIJIS framework that is subject to collation and analysis is criminal justice information, as defined and described in the HIJIS Privacy Policy.

3. Information accessed through the HIJIS framework by the **DPAMC** is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention, law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the agency.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities.

4. The **DPAMC** requires that all analytical products be reviewed and approved by the agency's administrative staff to ensure that they provide appropriate privacy protections prior to dissemination or sharing by the agency.

Merging Records

1. Information received by the **DPAMC** through the HIJIS framework will be merged only by authorized individuals who have been trained accordingly.

2. Records about an individual or organization received through the HIJIS framework from two or more sources will not be merged by the **DPAMC** unless there is sufficient identifying information to clearly establish that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

3. If the matching requirements are not fully met but there is reason to believe the records are about the same individual, the information may be associated by the **DPAMC** if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

Sharing and Dissemination

1. Information accessed through HIJIS by the **DPAMC** may be disseminated within the agency in the performance of official duties in accordance with applicable laws and procedures. An audit log sufficient to allow the identification of each individual who received information accessed by the agency through HIJIS and the nature of the information should be kept by the agency.

2. Information and records retained by the **DPAMC** may be disclosed **to a member of the public** with the written authorization of the providing agency, only if the information is defined by law to be a public record or otherwise appropriate for release to further the agency's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the agency for this type of information. An audit log sufficient to allow the identification of each individual member of the public who received information retained by the agency and the nature of the information should be kept by the agency but may be disclosed only in connection to a challenge to the legitimacy of the disclosure itself but not for investigatory or other criminal justice purposes.

3. Information accessed through HIJIS and records retained by the **DPAMC** may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access, only for those uses and purposes specified in the law, and with the written authorization of the providing agency. An audit log sufficient to allow the identification of each individual who requested, accessed, or received information retained by the agency; the nature of the information requested, accessed, or received; and the specific purpose will be kept by the **DPAMC**.

4. Information accessed through HIJIS and records retained by the **DPAMC will not** be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior authorization from or notice to the originating agency that such information is subject to disclosure or publication.
   - Disseminated to persons not authorized to access or use the information.

5. There are several categories of records that may be shared through HIJIS that originating agencies will ordinarily not provide to the public:
   - Records required to be kept confidential by law are exempted from disclosure requirements.
   - Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in

accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement entities that are exempted from disclosure requirements. However, certain law enforcement records must be made available for inspection and copying under Rule 16 of the Hawaii Rules of Penal Procedure.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- A violation of an authorized nondisclosure agreement.

6. The **DPAMC** shall not confirm the existence or nonexistence of information, accessed or shared through HIJIS, to any person or agency that would not be eligible to receive the information unless otherwise required by law.

Redress

Disclosure

1. If authorized by rule or statue, upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the **DPAMC**. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The agency's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available by the **DPAMC** to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23 (see 28 CFR § 23.20(e)).
   - The information source does not reside with the agency.
   - The agency did not originate and does not have a right to disclose the information.
   - Other **authorized** basis for denial.

3. If the information does not originate with the agency, the requestor will be referred to the originating agency, if appropriate or required, or the agency will notify the source agency of the request and its determination that disclosure **by the agency** or referral

of the requestor to the source agency was neither required nor appropriate under applicable law.

Corrections

1. If an individual requests correction of information *originating with the **DPAMC*** that has been disclosed to the individual, the agency's **administrative staff** or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

Appeals

1. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the **DPAMC** or the originating agency. The individual will also be informed of the procedure for appeal when the agency or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

Complaints

1. If an individual has a complaint with regard to the accuracy or completeness of protected information that:
    (a) Is exempt from disclosure.
    (b) Has been or may be shared through the HIJIS framework.
        (1) Is held by the **DPAMC**, and
        (2) Allegedly has resulted in demonstrable harm to the complainant (e.g. denial of employment due to an incorrectly assigned warrant or erroneous disposition).

    The DPAMC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints may be submitted to the Prosecuting Attorney at 150 South High Street, Wailuku, Hawaii 96793. The **DPAMC** will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information accessed or retained by the **DPAMC** from the HIJIS framework to the complainant unless otherwise required by law.

    The **DPAMC** will flag the record within the **DPAMC** system such that it will not be accessible through HIJIS. The **DPAMC** will then either purge the information so that it will not be accessible through HIJIS or correct any identified data/record deficiencies or verify that the record is accurate prior to enabling the record to be accessible through HIJIS. All information shared through HIJIS that is the subject of a complaint will be reviewed by the **DPAMC** within 30 days. If there is no resolution within 30 days, the **DPAMC** will not enable the record to be accessible through the HIJIS framework until such time as the complaint has been resolved and the record corrected or confirmed to be accurate. A record will be kept by and the **DPAMC** of all complaints and the resulting action taken in response to the complaint.

If the **DPAMC** is not the source of the record, the **DPAMC**'s administrative staff will notify the Originating entity in writing or electronically within 14 days of receipt of the complaint and, upon request by the **DPAMC**, the Originating entity will flag the record within the Originating entity's system such that it will not be accessible through HIJIS. The Originating entity will then either purge the information so that it will not be accessible through HIJIS or correct any identified data/record deficiencies or verify that the record is accurate prior to enabling the record to be accessible through HIJIS. All information shared through HIJIS that is the subject of a complaint will be reviewed by the Originating entity within 30 days. If there is no resolution within 30 days, the Originating entity will not enable the record to be accessible through the HIJIS framework until such time as the complaint has been resolved and the record corrected or confirmed to be accurate. A record will be kept by and the Originating entity of all complaints and the resulting action taken in response to the complaint.

Security Safeguards

1. The **DPAMC** is designated and trained to perform or oversee the performance of the **DPAMC**'s security functions as defined in this section.

2. The **DPAMC** will operate in a secure facility protected from external intrusion. The agency will utilize secure internal and external safeguards against network intrusions. Access to the agency's databases from outside the facility will be allowed only over secure networks.

3. Access to **DPAMC** information, that will be shared through the HIJIS framework, will be granted only to the agency personnel whose positions and job duties require such access and who have been trained accordingly.

4. Queries made to the **DPAMC**'s data applications should be logged into the data system identifying the user initiating the query.

5. The **DPAMC** should utilize logs to maintain audit trails of requested and disseminated information.

6. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data or with data shared through HIJIS.

Information Retention and Destruction

1. All applicable information that may be shared by a participating agency through the HIJIS framework or is obtained through HIJIS and retained by a receiving participating agency will be reviewed by the retaining agency for record retention (validation or purge) as specified by the agency's retention schedule.

2. When information accessed or shared through HIJIS has no further value or meets the criteria for removal according to the **DPAMC**'s retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency and made inaccessible through HIJIS.

3. The **DPAMC** will delete information, accessed or shared through HIJIS, or return it to the originating agency once its retention period has expired as provided by the HIJIS Privacy Policy, as well as the **DPAMC** HIJIS Privacy Policy, or as otherwise agreed upon with the originating agency in a participation or membership agreement.

4. No approval will be required from the originating agency before information that is accessed through HIJIS and held by the **DPAMC** is destroyed or returned in accordance with the agency's retention schedule.

5. Notification of proposed destruction or return of records obtained through the HIJIS framework may or may not be provided to the originating agency by the **DPAMC**, depending on the relevance of the information and any agreement with the originating agency.

6. A record of information to be reviewed for retention will be maintained by the **DPAMC**, and for designated system(s) accessible through HIJIS.

7. A printed or electronic confirmation of the deletion will be provided to the originating agency when required under law or if part of the terms of a pre-established agreement with the agency.

Accountability and Enforcement

Information System Transparency

1. The **DPAMC** will be open with the public in regard to information collection practices. The HIJIS Privacy Policy, as well as the **DPAMC** Privacy Policy, will be provided to the public for review, made available upon request, and posted on the **DPAMC**'s Web page at the Maui County website: www.http://co.maui.hi.us.

2. The **DPAMC**'s administrative staff will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information accessed through HIJIS and retained by the agency and any information originated and maintained by the agency which is accessible through HIJIS. The administrative staff can be contacted at 150 South High Street, Wailuku, Hawaii 96793.

Accountability

1. Queries made to the **DPAMC**'s data applications should be logged into the data system identifying the user initiating the query.

2. The **DPAMC** should maintain an audit trail of accessed, requested, or disseminated information disseminated. An audit trail should be kept for a minimum of one (1) year of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The **DPAMC** should adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of the HIJIS Privacy Policy, as well as the **DPAMC** Privacy Policy and applicable law. This will include logging access to agency-owned systems and periodic auditing, so as to not establish a pattern of the audits. These audits should occur at least **annually**, and a record of the audits will be maintained by the Information Technology Systems Division of the Department of Management.

4. The **DPAMC**'s personnel or other authorized users should report errors and suspected or confirmed violations of the HIJIS privacy policy, as well as the **DPAMC** Privacy Policy relating to protected information to the **DPAMC**'s records management system.

5. The **DPAMC** should annually conduct an audit and inspection of the information contained in its information system(s) that is shared through the HIJIS framework. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the agency's information system(s).

6. The **DPAMC**'s administrative staff should review and update the provisions protecting privacy contained in this HIJIS Privacy Policy **annually** and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

Enforcement

1. If participating agency personnel or an authorized user is suspected or found to be in noncompliance with the provisions of the HIJIS Privacy Policy, as well as the **DPAMC** Privacy Policy, regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Prosecuting Attorney of the **DPAMC** will:
   - Suspend or discontinue access to information by the agency personnel or the authorized user.
   - Suspend, demote, transfer, or terminate agency personnel, as permitted by applicable personnel policies.
   - Apply administrative actions or sanctions as provided by applicable rules and regulations or as provided in agency/agency personnel policies.

- If the authorized user is from an agency external to the agency, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The **DPAMC** reserves the right to restrict the qualifications and number of personnel having access to agency information and to HIJIS and to suspend or withhold service and deny access to any participating agency personnel or authorized user violating the HIJIS Privacy Policy, as well as the **DPAMC** Privacy Policy.