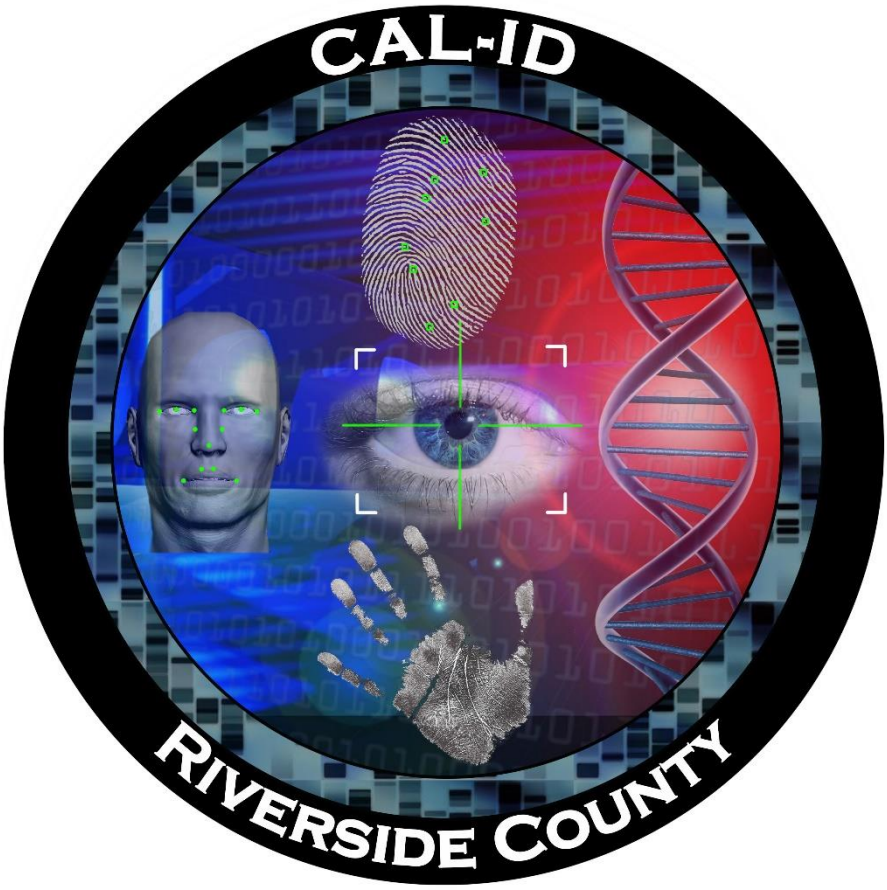

MOBILE ID POLICY

October 24, 2023

Table of Contents

A. Preface

This policy has been developed by Riverside County Cal-ID (CALID) and is approved for use and publication by the Riverside County Sheriff's Department (RCSD). CALID acknowledges it lacks authority to write policy for individual law enforcement agencies who may utilize CALID's mobile identification (Mobile ID) program and devices. However, CALID is responsible for the governance, oversight and operation of its Mobile ID system and the application and devices which it provides to the law enforcement agencies in Riverside County. This policy shall be used as the foundation for those agencies that choose to utilize CALID Mobile ID. This policy is intended for CALID personnel and any authorized law enforcement personnel utilizing Mobile ID. Participating agencies may choose to implement their own policy or impose greater restrictions on their employees' use of CALID Mobile ID as desired. Subsequent agency policy shall not override this policy and all users of CALID Mobile ID shall be bound by this policy. CALID retains exclusive rights to limit or prohibit an individual or agency's use of Mobile ID as warranted.

B. Purpose Statement

The CALID program has provided a Mobile ID application and devices to authorized RCSD and CALID participating agency personnel to assist in determining the identity of an individual who cannot produce proper identification, who produces identification that appears to be illegitimate, who lacks the capacity or ability to identify themselves and who are a danger to themselves or others, or are deceased.

CALID has established access and use of Mobile ID to support the efforts of law enforcement and public safety agencies within Riverside County. The DataWorks Plus Mobile ID software application resides in and is managed by CALID. Mobile fingerprint capture devices are provided and managed by CALID.

It is the purpose and intent of this policy to provide Riverside County law enforcement personnel with standards, guidelines, and recommendations for the access, use, dissemination, retention, and purging of information obtained by and applicable to the Mobile ID program. This policy will ensure that all Mobile ID uses are consistent with authorized purposes.

C. Policy Applicability and Legal Compliance

All deployments of the Mobile ID application are for official use only and information therein is considered law enforcement sensitive.

This policy was established to ensure that Mobile ID is used lawfully, and fingerprint images and search information is obtained, disseminated, retained, and purged appropriately. All CALID personnel and authorized users working in direct support of their unit or LE agency, personnel providing information technology services to CALID, and private vendors, will comply with this Mobile ID Policy. Participating agencies are encouraged to implement their own Mobile ID policy, however, it must incorporate the established usage and guidelines as described in Item D below, and will be in addition to, not in replacement of, this policy.

D. Use of Mobile ID

Access to or disclosure of Mobile ID search results will be provided only to those individuals who are authorized to have access, for legitimate law enforcement purposes only, and to CALID personnel charged with the responsibility for system administration and maintenance.

CALID issued Mobile ID devices are used to capture fingerprints to verify a subject's identity through the CALID Automatic Fingerprint Identification System (AFIS). Additionally, an identity search of the California Department of Justice's (DOJ) fingerprint repository as well as the FBI's Repository of

Individuals with Special Circumstances (RISC) can be conducted with the mobile fingerprint scanner. At no time will a user capture fingerprints for a Mobile ID search outside of their official law enforcement duties. Mobile ID shall not be used for random or general investigative or intelligence gathering.

CALID has established that Mobile ID may be used during a legal detention or arrest in the following circumstances:

- The individual does not possess or is unwilling to provide valid identification.
- There is a doubt of the authenticity of any identification that is presented.
- An individual is driving a motor vehicle and does not possess a valid driver's license.
- An identification is required per agency policy prior to issuing any citation/s.

CALID has established the following guidelines for Mobile ID searches:

- Authorized RCSD and participating LE agency personnel may utilize the Mobile ID application only on department/agency authorized and managed mobile devices (MDC, GTAC, etc.).
- Users are required to log in and be authenticated into the DataWorks Plus Mobile ID system using their RCSD credentials or Cal-Photo credentials.
- Mobile searches shall only be performed during the course of LE personnel's lawful duties.
- Prior to utilizing a Mobile ID device, LE personnel should first attempt to ascertain an individual's identity by means other than a fingerprint search, such as requesting identification, e.g., state issued driver's license or identification card.
- Prior to capturing an individual's fingerprints, LE personnel must have lawful detainment or meet the "No Consent" criteria described as:
    - Individuals who lack the capacity or ability to identify themselves and who are a danger to themselves or others.
    - Those individuals who are deceased and not otherwise identified.
- At no time is the use of force permitted to capture a subject's fingerprint during field detainment.
- Mobile ID is only an aid to the identification of a person. Information received from Mobile ID shall be used to compare, evaluate and/or corroborate information obtained through other investigative methods.
- Mobile ID shall not be used as the sole grounds for establishing probable cause for arrest.
- Mobile ID searches are recommended for field citation releases.
- If LE personnel are not satisfied with the results of the Mobile ID search, they shall follow department/agency protocols as if a Mobile ID device was not available.

E. Sharing and Disseminating Mobile ID Information

California DOJ's CORI Information Bulletin 13-04-CJIS cites California Penal Code 11105 which identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions."

Mobile ID search information will not be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by CALID's agreement with a commercial vendor.

- Disclosed to unauthorized individuals or for unauthorized purposes.

F. Disclosure Requests

CALID will disclose Mobile ID program information to the public in accordance with DOJ's CORI Information Bulletin 13-04-CJIS, the RCSD Media Information Bureau (MIB), and/or the RCSD Information Services Bureau (ISB) policy when applicable. Additionally, California Public Records Act (CPRA) requests may be made to the CPRA unit via the official RCSD website or emailing CPRA@riversidesheriff.org. CALID will work jointly with the Department's CPRA unit and participating agencies in receipt of a CPRA request to provide the requested information. CALID will keep a record of all information provided to the CPRA unit to comply with requests and the CPRA unit will keep a record of what information is disclosed.

G. Security and Maintenance

CALID will comply with DOJ CJIS and RCSD Technical Services Bureau security policies, to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity.

Authorized access to the Mobile ID system will be granted only to LE personnel whose positions and job duties require such access and who have successfully completed a background check through their agency.

All Mobile ID equipment and software will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

CALID and the Mobile ID vendor, will store information in a manner that ensures that it cannot be accessed or purged except by personnel authorized to take such actions.

H. Information Retention and Purging

Mobile ID searches/responses are stored on CALID servers for two years, then purged. Searches on individual device applications are stored until the maximum number of searches for the local queue has been reached, typically 25 searches. The oldest searches will then purge as new searches are created.

I. Accountability and Enforcement

CALID will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the Mobile ID system requirements and with the provisions of this policy. This will include logging access to Mobile ID information, may include any type of medium or technology (e.g., physical servers and mobile devices) used in a work-related activity, and may entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions.

CALID personnel or other authorized users shall report errors, malfunctions, or deficiencies of the Mobile ID program and suspected or confirmed violations of the Mobile ID policy to the appropriate RCSD personnel, the CALID Manager, or designee.

The CALID Manager, or designee, will review and update the provisions contained in this Mobile ID policy as needed and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the Mobile ID system. RCSD Administration reserves final decision-making authority of the Mobile ID policy.

If CALID personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy, the CALID Manager will:

- Suspend or discontinue access to the Mobile ID system by the participating agency, or the authorized user.
- Notify the agency Department head of the suspected violation and initiate appropriate disciplinary/administrative actions, following a thorough review of the alleged policy violations.
- Refer the matter to agency criminal investigators for investigation and review to determine if criminal prosecution is appropriate.

CALID reserves the right to establish the qualifications and number of personnel having access to the Mobile ID system and to suspend or withhold service and deny access to any participating LE agency or participating LE agency personnel violating this policy.

J. Definitions

Access—Information access is being able to retrieve particular information, usually requiring permission to use. Web access means having a connection to the internet through an access provider or an online service provider.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes, but which is not available to everyone.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, or federal agency with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement (LE) Personnel—Any person employed, appointed, or elected in any way to a position within a law enforcement agency**.**

Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Search—For the purposes of Mobile ID, the act of sending a fingerprint image through a fingerprint repository for identification.