HOWARD COUNTY DEPARTMENT OF POLICE

GENERAL ORDER ADM-67
EVIDENCE.COM

EFFECTIVE AUGUST 30, 2022

This General Order contains the following numbered sections:

I. POLICY

It is the policy of the Howard County Department of Police (HCPD) to maintain a database for case management. Evidence.com is a cloud-based evidence management platform that is utilized by the HCPD as the system to store and manage digitally encrypted data in a highly secure environment accessible to personnel based on security clearance.

II. DEFINITIONS

A. Evidence.com: A digital file management website that securely stores digital photographs, body worn camera videos, and other forms of digital media.

B. System Administrator: The Laboratory Director of the Forensic Sciences Division (FSD) assigned as the administrator of HCPD's Evidence.com database. This member is granted full access to user rights.

C. Digital Evidence: Any record of a digital file from an electronic source. This includes video, audio, photographic, and its associated metadata.

D. Audit Trail: A chain of custody on Evidence.com that details the transactions associated with any use of the system.

E. Auto Tag: The addition of metadata to an individual body worn camera video file that is automatically generated based on integrated system data between the Records Management System (RMS) system and Evidence.com.

F. Axon Capture: The Axon Capture application is available for users with an Evidence.com profile. The application is utilized by members to upload photos, video, and audio evidence directly to Evidence.com along with the ability to add the IR#, retention categories, and sync metadata. Digital Evidence is directly uploaded to Evidence.com via the member's individual profile.

G. Axon Citizen: The Axon Citizen application is available for users with an Evidence.com profile. The application is utilized by members to request photos, video, and audio evidence from Community Members. Digital Evidence is directly uploaded to Evidence.com via the member's individual profile.

H. Axon Respond: The Axon Respond application allows members with permission to view officer locations on a map and/or view live streams in real-time when the Body Worn Camera (BWC) is activated in Event Mode. It does not permit a BWC to be pinged for GPS data or to remotely activate Event Mode.

I. Axon View: The Axon View application supports BWC operation only. Axon View securely pairs through Bluetooth with a particular member's BWC. Axon View pairs through a computer USB connection. The application allows the user to remotely review and add the IR# and retention category

to the recorded video stored with a paired BWC prior to docking for upload. Axon View does not collect or store any evidence to a device.

J. Smart Phone: A departmentally issued mobile computer device enabled with cellular connection, internet access, and an operating system capable of running downloaded applications.

III. DEPARTMENTALLY ISSUED DEVICES

A. Body Worn Cameras (BWC)

1. Members of the HCPD are authorized to wear and utilize BWC in the course of their duties as detailed in General Order ADM-31, Body Worn Cameras.

2. All BWC data shall be docked daily in order for footage to upload to Evidence.com.

B. Smart Phones

All sworn members shall be issued a Smart Phone for use as their Departmental camera. Reference General Order ADM-41, Smart Phone Procedures.

C. Digital Cameras – Authorized for Specific Sections only[1]

1. The following Sections shall be permitted to use Departmentally issued Digital Cameras:

a. Forensic Sciences Division

b. Traffic Management Division

c. Internal Affairs Division

d. Criminal Investigations Command

e. Other Units as designated by the Chief of Police

2. Each Digital Camera will be issued with at least two (2) media cards. A spare set of batteries will be kept with the Digital Camera at all times.

3. Each Division/member assigned a Digital Camera will be responsible for the care, maintenance, and security of the camera and shall maintain the camera in a state of operational readiness.

4. The correct date and time shall be properly set within the Digital Camera.

5. Only one case shall be photographed per media card. HCPD Form 1312, Digital Media Envelope, shall serve as the photo identifier card. It shall be completely filled out and shall be the first photo taken for the case.

a. If multiple locations are involved in a single crime scene, a photo identifier that clearly delineates the new location shall be photographed to divide the images or the additional crime scene can be photographed with a separate media card.

b. Before removing a media card from the Digital Camera, the Digital Camera must be turned off as a loss of data may occur.

c. The media card shall be submitted in the HCPD Form 1312, Digital Media Envelope, that was photographed as the identifier card. The submitting officer shall secure the

1 CALEA 83.2.2A

envelope closed with blue evidence tape across the entire width of the envelope seal and write their initials and the date across the tape seal.

d. The officer shall enter the submission in the Media Card Logbook and then place the envelope in the locked Media Card drop box.

6. When photographing victim injuries, both facial and full body photographs shall be taken to establish context and identity. If possible, injury photographs shall be taken both with and without scale using the scale on the HCPD Form 1312, Digital Media Envelope.

7. Upon receipt by the Forensic Sciences Division (FSD), the media will be downloaded, and the media card will be returned to the submitting officer. The officer shall be responsible for reformatting the media.

8. HCPD Form 1310, Digital Photo Submission Form, shall be completed by the Crime Scene Technician downloading the images and forwarded to the Records Section.

D. Other Devices

Any member utilizing a device not referenced above that interfaces with Evidence.com shall follow all applicable policies related to evidence management.

IV. PROCEDURE

A. Members will be trained in the utilization of Evidence.com based on their assignment.

B. Members are prohibited from using personally owned digital devices for recording, transmitting, duplicating, or storing Digital Evidence of crime scenes, traffic stops, interactions with citizens, or any investigative or police action, unless authorized by a supervisor under exigent circumstances.[2]

1. The supervisor shall be responsible for ensuring appropriate data transfer in accordance with General Order OPS-41, Smart Phone Procedures, and file deletion from the member's personal device.

2. If Digital Evidence is taken on a personal device, it shall be noted in the incident report.

C. When not using the Axon Capture app, any photo taken or text message generated in relation to an incident report on the Smart Phone shall be uploaded to Evidence.com under the appropriate IR# and then deleted from the device.

To upload:

1. Open the Axon Capture app.

2. Click Import.

3. Select photos from gallery.

4. Select Done.

5. Complete the ID Field: Enter the 9 Digit IR# in the ID Field (Example: 220012345).

6. Title Field: The file name of any media shall not be altered. The file name assigned by the Axon Capture app shall be the permanent name of that file.

7. Complete the Category: Assign a Retention Category from the drop-down list. This category

2 CALEA 83.2.2D

shall be the same as the offense used on the member's report in the Records Management System (RMS) system.

D. Members are prohibited from sharing any Digital Evidence internally unless it is for official work purposes.

E. This policy does not prohibit the Forensic Sciences Division (FSD) and decentralized mobile examiners from transmitting data to and from authorized entities.

F. Submission of Evidence:

1. Body Worn Camera (BWC)

a. Members shall submit BWC evidence in accordance with General Order ADM-31, Body Worn Cameras.

b. Evidentiary copies of Digital Evidence will be accessed from Evidence.com using departmentally approved equipment and for law enforcement purposes only.

2. Axon Capture

a. Members shall utilize the Axon Capture application on their Smart Phone as the primary method of taking photographs, video recordings, or audio recordings.

b. Axon Capture will be accessed by members via their Smart Phone. Use of the application on unauthorized devices is strictly prohibited.

c. All media recorded shall be uploaded through the application into Evidence.com. Once uploaded, no files shall be deleted from Evidence.com except by authorized personnel in accordance with the scheduled retention periods.

d. When uploading images, videos or audio through the Capture app into Evidence.com, the member shall:[3]

i. Complete the ID Field: Enter the 9 Digit IR# in the ID Field (Example: 220012345)

ii. Title Field: The file name of any media shall not be altered. The file name assigned by the Axon Capture application shall be the permanent name of that file.

iii. Complete the Category: Assign a Retention Category from the drop-down list. This category shall be the same as the offense used on the member's report in the Records Management System (RMS).

iv. Any time photographs are taken and submitted, it must be noted in an incident report.

3. Photographs may only be taken directly on the Smart Phone and not through Axon Capture when there is an immediate need, for example, to help identify an individual.

a. Any photographs taken on the Smart Phone **must** be uploaded to Evidence.com.

3 CALEA 83.2.2B; 83.2.2C

b. Once the upload is confirmed, the photograph shall be deleted from the Smart Phone's photo gallery.

4. Axon Citizen

a. Members can utilize Axon Citizen to send an invitation to a community member through the application or from the Evidence.com web browser.

b. Members may not send a link to themselves to upload items. All media items removed by members must be uploaded into Evidence.com either through Axon Capture or through submission to the Photo Dropbox (photos) and/or Property (videos).

c. When inviting a community member to submit media, the member shall:[4]

i. Complete the ID Field: Enter the 9 Digit IR# in the ID Field (Example: 220012345)

ii. Complete the Category: Assign a Retention Category from the drop-down list. This category shall be the same as the offense used on the member's report in Records Management System (RMS).

iii. Select a Delivery Method: Text or Email. Follow the prompts to complete the community members information.

d. Once the invitation is sent, the community member will get a notification allowing them to upload the media. If it expires, the member will need to send an additional invite if necessary to recover the media.

e. Once media is submitted, the member will receive an email notification. The member shall review each file no later than ten (10) days after notification, and either accept or reject the media. It is the member's responsibility to review and verify the content of all media prior to accepting it.

f. Any time an invitation is sent or evidence is received, it must be noted in an incident report.

5. Small Unmanned Aircraft Systems (sUAS)

The HCPD will utilize sUAS to provide an aerial visual perspective in responding to emergency situations and exigent circumstances. The collection and use of any audio/video recordings or other data originating from or generated by the sUAS will be utilized in compliance with General Order OPS -53, Small Unmanned Aircraft Systems.

6. 911 Recordings

a. Request for 911 recordings shall be made through the Information Management Division or Communications Division.

b. Responses to requests for recordings and supplemental documentation shall be uploaded to Evidence.com.

c. The Information Management Division shall be responsible for responding to all

4 CALEA 83.2.2A; 83.2.2B; 83.2.2C

requests.

G. The Information Management Division shall be responsible for:

1. Responding to Freedom of Information Act (FOIA), or the Maryland Public Information Act (MPIA) requests, and subpoenas in compliance with all federal, state, and local laws regarding public record release.

2. Forwarding Digital Evidence to the State's Attorney's Office (SAO) for case management and prosecution upon request.

H. The Forensic Sciences Division (FSD) shall be responsible for forwarding Digital Evidence to the State's Attorney's Office (SAO) for case management and prosecution upon request.

V. ACCESS, REVIEW, AND USE OF RECORDINGS

A. All Digital Evidence is the property of HCPD.

B. Access to Digital Evidence shall be granted to authorized users only. It is the responsibility of authorized users to keep their username and password confidential. Accessing, copying, or releasing any Digital Evidence is strictly prohibited, except as required by law or as part of an official law enforcement investigation. The following categories are non-legal administrative terms specific to Evidence.com:

1. Unrestricted Evidence: All members shall have the ability to view and access Unrestricted Evidence for report writing and/or training purposes.

2. Restricted Evidence: Lieutenants and above shall have the ability to view and access Restricted Evidence.

3. Confidential: The Chief, Majors and designated members of the Internal Affairs Division shall have the ability to view and access Confidential Evidence.

4. Administrators and members of the Body Worn Camera Division shall have full rights to all evidence but shall only view evidence that is required in the completion of their job duties.

C. Axon Respond: In accordance with General Order ADM-31, Body Worn Cameras, all sworn members shall have access to Axon Respond. All sworn members shall have access to GPS data.

D. Digital Evidence may be utilized by the Department for HCPD education and training purposes with approval of the Body Worn Camera Division Commander.

E. Members outside of the Information Management Division and the Forensic Sciences Division (FSD) shall not edit, alter, erase, duplicate, copy, or share Digital Evidence outside of HCPD.

F. The HCPD Office of Public Affairs shall have access to list evidence in Evidence.com. Requests to view specific files shall be made through the Information Management Division.

G. Personnel in the Office of Law (OOL) may review Digital Evidence for the defense of the Department in civil litigation matters or at the issuance of a Legal Hold.

H. BWC Compliance Reviews: Watch Commanders or Division Commanders shall utilize Axon Performance for BWC quality assurance reviews in accordance with General Order ADM-31, Body Worn Cameras.

I. Authorized members of the Communications Division shall have the ability to perform certain functions in Evidence.com:

1. Designated Emergency Communications Supervisors (ECS) shall have permission to utilize Axon Respond to access live GPS locations and stream live video from a BWC when directed by an Incident Commander (Lieutenant or above).

2. Dispatchers shall be able to view GPS data.

3. Authorized personnel shall be able to upload 911 Recordings and supplemental documentation to Evidence.com.

VI. RETENTION OF DIGITAL EVIDENCE

Retention Periods

A. Digital Evidence will be kept for at least the minimum time required under all applicable laws, policies, and the defined legal retention schedule approved by the State Archives.

B. Retention periods may be extended for judicial, or litigation holds only. The Information Management Division or the Forensic Sciences Division (FSD) shall be the only entities to extend the retention period.

C. Any data uploaded to Evidence.com shall be retained in accordance with the appropriate HCPD retention schedule.

VII. EXTERNAL RELEASE OF DIGITAL EVIDENCE

A. Only the Information Management Division shall have the ability to share Digital Evidence with external customers. All external requests for Digital Evidence must be made in writing. The request shall include the name and contact information of the requestor. The established fees must be submitted prior to the release of requested records, if required.

B. The HCPD Custodian of Records shall make the final determination on releasing any Digital Evidence, consistent with the Freedom of Information Act (FOIA), the Maryland Public Information Act (MPIA), and other applicable State and Federal statutes and regulations.

C. The Forensic Sciences Division (FSD) shall have the ability to share Digital Evidence with the Howard County States' Attorney's Office. All requests must be made in writing using HCPD Form 1302, SAO request form.

D. The HCPD Office of Public Affairs may be authorized by the Chief of Police to post or share properly redacted video as appropriate.

E. Members are prohibited from sharing any Digital Evidence outside the Howard County Police Department. Requests for access from external customers shall be made through the Information Management Section.

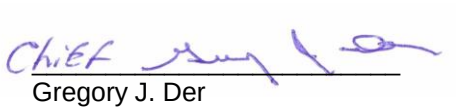
VIII. PROGRAM MAINTENANCE

A. The Laboratory Director of the Forensic Sciences Division will serve as Administrator for the Evidence.com database and user access.

B. The Body Worn Camera Division shall maintain the hierarchy structure within Evidence.com and shall be responsible for reassigning sworn members to the appropriate roles and permissions upon hire, transfer, promotion and separation from the Department.

C. The Body Worn Camera Division shall be responsible for the distribution, training and maintenance of all Department-issued Smart Phones and body worn camera devices.

AUTHORITY:



Gregory J. Der
Chief of Police