

# Healthcare Privacy Considerations of Body-Worn Cameras

Save to myBoK

By Dana DeMasters, MN, RN, CHPS, and Deanna Peterson, MHA, RHIA, CHPS

A police officer with a body-worn camera records video of an altercation in an emergency department involving a patient who has become violent. During the recording another patient not involved in the altercation has their image captured. The officer leaves the facility with the images. Is this a breach? What are the next steps for the covered entity (CE)?

Recent high-profile cases centered on police actions, such as those in Ferguson, MO, and New York, have spurred an outcry from citizens, media, and law enforcement agencies to require law enforcement officials to use body-worn cameras. Body-worn cameras have the ability to collect video surveillance and may include video glasses, helmet cameras, shoulder microphone/cameras, and cameras worn on the chest. The cameras may be worn by traditional law enforcement officers at the city, state, and county levels but may also be utilized by a CE's security guards. While studies have shown that body-worn cameras may reduce the use of police force and citizen complaints, there are no consistent regulations governing their use.<sup>1</sup>

## Recent Camera Legislation Vague on Privacy

Prior to 2015, only four states had laws concerning body-worn cameras: Pennsylvania, Vermont, Oklahoma, and New Hampshire. However, in 2015 most states considered legislation about body-worn cameras and how they should be implemented and managed. Laws were passed in California, South Carolina, Nevada, and New Jersey requiring their use by certain law enforcement officers. Other states—Arizona, Colorado, Louisiana, Maryland, and Vermont—passed legislation to study the topic while some states “delegated the issue to local municipalities and police departments” in Alaska, Maine, West Virginia, and Wyoming, according to an article in *Fiscal Note*.<sup>2</sup>

Some lawmakers, police, and privacy advocates promote restrictions about the release of audio and video recordings, while freedom of information advocates feel restrictions undermine a key purpose of the recordings—to hold law enforcement accountable for their actions. Debate also exists concerning whether open record laws (state laws regulating use and disclosure of government agency documents) should apply to video recordings by law enforcement, and if current state and federal privacy laws are adequate to protect the release of these recordings. For example, the Freedom of Information Act, Exemption 7(C) protects from disclosure records for law enforcement purposes, only to the extent that the records “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”<sup>3</sup> Furthermore, HIPAA privacy and information security laws will factor into these incidents as CEs must safeguard protected health information (PHI) in any medium, including the storage and release of PHI.

## Current Body-Camera Practice

There are differing recommendations for when law enforcement agencies should record encounters. For instance, the Police Executive Research Forum (PERF) recommends only activating cameras when responding to a call or during police activity such as arrests and pursuits.<sup>4</sup> PERF further elaborates that officers have some discretion as to when to activate the camera and that agency policy should dictate these situations. Conversely, the American Civil Liberties Union (ACLU) originally recommended recording all encounters and notifying a subject that the encounter is being recorded.<sup>5</sup> Recently, the ACLU revised their position to record “when responding to a call for service or at the initiation of any other law enforcement or investigative encounter between a police officer and a member of the public.”<sup>6</sup>

Moreover, some agencies have adopted policies that allow officers to turn off cameras to avoid privacy violations.<sup>7</sup> CEs should attempt to work closely with law enforcement to understand each agency's use of body-worn cameras and assist them in understanding the CE's policies about the use of body cameras in their facilities.

In addition to the challenge of balancing differing recommendations about when to record encounters, law enforcement must acquire adequate staff, technology, and other resources to manage the cameras and set guidelines for data storage, redaction, and release of images. Camera footage can be classified as evidentiary (possibly containing footage to be used in an investigation) and non-evidentiary (footage that would not aid in an investigation). Non-evidentiary footage retention is typically governed by agency policy and may range from seven days to one year while evidentiary footage is governed by state law and may be retained for a longer time—potentially indefinitely (i.e., homicide).<sup>8</sup> Facilities should also be aware that some police departments may outsource their video evidence to private companies, which may include cloud storage, raising further concerns about protecting the data.

## Develop Policies and Procedures

Given the disparity of law enforcement agency practice and pending state legislation, CEs may struggle with how to manage the body-worn camera scenario as described above. It is possible that this scenario may be classified as an incidental disclosure as the recording of the other patient could not have “reasonably” been prevented and, therefore, is not a breach. On the other hand, if the CE was aware the officer was recording, could steps have been taken to minimize the PHI recorded? The question must be answered as to whether or not it is “reasonable” to limit the recording of PHI by law enforcement, particularly when facilities are aware that body-worn cameras are in use. Furthermore, HIPAA does allow for release to law enforcement agencies in circumstances where there is an imminent threat to the individual or public.<sup>9</sup>

However, some state laws may be more stringent and require reporting. Therefore, it is important for CEs to review all applicable regulations and develop policies and procedures to handle body-worn cameras. It is advisable to involve legal counsel when examining all applicable laws. At minimum, consider the following when drafting a policy on body-worn cameras:

- Determine the CE’s position on recording and body-worn cameras—for example, request that officers have cameras turned off when entering the facility.
- Identify the multiple law enforcement agencies that may interact with the facility (i.e., county, city, state, in-house security guards) and obtain information about their recording policies.
- Notify agencies and officers regarding CE’s body-worn camera policy, for example, through in-person meetings with local police, sending letters of explanation and copies of policy to agencies, and posting “no video” signage at facilities.
- Assess areas of the facility where law enforcement may enter.
- Educate staff about the CE’s policy and the importance of notifying the CE’s privacy or compliance officer when a recording happens.
- Utilize a tool for staff to gather information and document in the patient’s record when a law enforcement recording occurs.<sup>10</sup>
- In addition to normal breach assessment and investigation procedures, when a recording occurs involving PHI, pay special attention to the assessment of any third party vendors used by law enforcement for video storage, redaction, and release.

As more states pass body-worn camera legislation, the guidelines for use, retention, and release may become clearer. Regardless, CEs should be proactive in collaborating with potential users of body-worn cameras to define proper uses that protect patient privacy.

## Notes

[1] Ariel, Barak and William A. Farrar et al. “The Effect of Police Body-Worn Cameras on Use of Force and Citizens’ Complaints Against the Police: A Randomized Controlled Trial.” *Journal of Quantitative Criminology* 31, no. 3 (September 2015): 509-535 <http://link.springer.com/article/10.1007%2Fs10940-014-9236-3>.

[2] Brown, Rebecca. “Nearly all states considered police body cameras in 2015, few enacted laws.” *Fiscal Note*. August 6, 2015. [www.fiscalnote.com/2015/08/06/nearly-all-states-considered-police-body-cameras-in-2015-few-enacted-laws](http://www.fiscalnote.com/2015/08/06/nearly-all-states-considered-police-body-cameras-in-2015-few-enacted-laws).

[3] United States Department of Justice. Freedom of Information Act website. [www.foia.gov](http://www.foia.gov).

[2] US Department of Justice Office of Community Oriented Policing Services, and Police Executive Research Forum. "Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned." 2014. [www.justice.gov/iso/opa/resources/472014912134715246869.pdf](http://www.justice.gov/iso/opa/resources/472014912134715246869.pdf).

[5] American Civil Liberties Union. "A Model Act for Regulating the Use of Wearable Body Cameras by Law Enforcement." 2015. [www.aclu.org/model-act-regulating-use-wearable-body-cameras-law-enforcement](http://www.aclu.org/model-act-regulating-use-wearable-body-cameras-law-enforcement).

[6] Stanley, Jay. "Police Officer Discretion in the Use of Body Worn Cameras." American Civil Liberties Union Free Future Blog. February 2, 2015. [www.aclu.org/blog/free-future/police-officer-discretion-use-body-worn-cameras](http://www.aclu.org/blog/free-future/police-officer-discretion-use-body-worn-cameras).

[7] US Department of Justice Office of Community Oriented Policing Services, and Police Executive Research Forum. "Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned."

[8] Ibid.

[9] US Department of Health and Human Services Office for Civil Rights. "HIPAA Privacy Rule 45 CFR 164.512(f); 164.502(j)" [www.hhs.gov/ocr/privacy/hipaa/understanding/summary/](http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/).

[10] DeMasters, Dana. "Responding to Requests from Law Enforcement Officials for Release of PHI" *Journal of AHIMA* 86, no. 5 (May 2015): 44-46. <http://bok.ahima.org/doc?oid=107640>.

Dana DeMasters ([dana.demasters@libertyhospital.org](mailto:dana.demasters@libertyhospital.org)) is privacy/security officer at Liberty Hospital in Liberty, MO. Deanna Peterson ([Deanna.Peterson@firstclasssolutions.com](mailto:Deanna.Peterson@firstclasssolutions.com)) is assistant vice president of health information consulting services at First Class Solutions, Inc., in St. Louis, MO.

---

**Article citation:**

DeMasters, Dana; Deanna, Peterson. "Healthcare Privacy Considerations of Body-Worn Cameras" *Journal of AHIMA* 87, no.2 (February 2016): 32-33.

---

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.