EMS Body-worn Camera Quickstart Guide:

Legal Considerations for EMS Agencies

Version 1.0

NEMSIS
BETTER DATA. BETTER CARE.

Page Wolfberg & Wirth
The National EMS Industry Law Firm®

Contents

Disclaimers

- This Guide is an overview. It is not intended to cover every possible legal and compliance issue concerning the use of body-worn cameras in emergency medical services (EMS).
- These materials are not formal legal advice. Please contact an attorney if you need formal legal advice.
- Use of this Guide does not create an attorney-client relationship or a professional consulting relationship between you or your agency and Page, Wolfberg, & Wirth, LLC.
- You must consult an attorney licensed in your jurisdiction concerning matters of state law.
- It is solely your agency's responsibility to remain compliant with all federal and state laws, which are subject to change.

Introduction

Page, Wolfberg & Wirth (PWW) was asked by the National EMS Information System (NEMSIS) Technical Assistance Center (TAC) to identify and generally outline threshold legal considerations for EMS agencies contemplating the use of body-worn cameras (BWCs). BWCs are not yet in widespread use in EMS nationwide, but interest is growing. Organizations that have employed BWCs have realized significant **benefits** from BWC use. For example, BWCs can:

- Visually document the patient's condition and behavior in real time;
- Promote EMS practitioner accountability;
- Capture illegal or unprofessional conduct;
- Record adherence to, or failure to follow, protocols;
- Record patient/practitioner interactions;
- Resolve complaints against EMS practitioners;
- Assist in quality improvement;
- Offer effective scenario-based training; and
- Serve as evidence in litigation or other disputes.

Key Legal Considerations

- **Federal HIPAA Standards**
- **State Invasion of Privacy Laws**
- **State Wiretap/Eavesdropping Laws**
- **State Open Records Laws**
- **Data Retention Requirements**
- **Body-worn Camera Policy**

EMS agencies must evaluate legal, financial, and other issues (*e.g.,* public perception, staff impact, potential union bargaining, etc.) to determine if BWCs are right for their organization. The legal considerations identified in this Guide are some of the key threshold issues that EMS agencies must tackle when implementing BWCs.

Federal HIPAA Standards

BWCs recordings in which patients can be identified contain **protected health information** (PHI)[1] under the Federal Health Insurance Portability and Accountability Act (HIPAA). HIPAA requires EMS agencies covered by HIPAA to safeguard PHI and only use and disclose PHI in accordance with the Privacy Rule.

EMS agencies must treat BWC recordings the same way they would patient care reports (PCRs) and other patient records.

Does HIPAA Permit Body-worn Cameras?

Yes. HIPAA permits EMS agencies to capture PHI with BWCs and to use BWC recordings for treatment, healthcare operations, and other reasons permitted by the Privacy Rule.[2] Often, EMS agencies use BWC records for healthcare operations[3] activities identified in HIPAA, including:

- Quality assessment and quality improvement (QA/QI);
- Developing clinical protocols and guidelines; and
- Evaluation of patient safety activities.

HIPAA does <u>not</u> require patient consent for your agency to use BWC recordings for treatment and healthcare operations.[4]

Your HIPAA Checklist for BWCs

- **Business Associate Agreements with Vendors That Store PHI.** Because BWC recordings contain PHI, EMS agencies must enter into a business associate agreement (BAA) with any vendor or cloud storage provider (CSP) that **maintains** BWC recordings. For example, many agencies do not store much of their patient information on their own servers.
  Instead, this patient information is stored on the server of an ePCR vendor or another CSP (such as Amazon Web Service). If your BWC videos are stored by a third party, you will need a BAA with the vendor or CSP. Many times BAA language is included in the end user license agreement with a vendor.

- **Encrypt BWC Recordings and Devices.** It is strongly encouraged that BWC recordings be encrypted[5] whenever they are being ***stored*** or ***transmitted.*** This includes encrypting all digital media (flash drives, internal device storage, etc.) and

[1] Protected health information is defined as any individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity. 45 CFR § 160.103.
[2] 45 CFR § 164.506.
[3] 45 CFR § 164.501.
[4] **State** law may require patient consent to record (as discussed in "State Consent Laws" section of this Guide).
[5] The Department of Health and Human Services (HHS) recommends using the following encryption processes: PHI at Rest - NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. PHI in Motion - NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

any local or cloud-based servers on which you maintain BWC recordings. Ask the vendor that will maintain your BWC recordings, and your IT professionals, to ensure BWC recordings are encrypted when being maintained or transmitted.

- **Properly Delete BWC Recordings.** When your agency permanently deletes BWC recordings[6], it must permanently destroy the recording so that the recording cannot be retrieved. [7] Simply deleting the BWC file locally or dragging it to a "Recycle Bin" will not permanently delete the file. Your IT professionals can assist with tips on destruction.

- **Establish Role-Based Access Controls to BWC Recordings.** You must restrict workforce member access to BWC recordings to legitimate, work related and HIPAA-permitted reasons. For example, field practitioners should only have access to BWC recordings if they are permitted by your agency to review recordings of their calls for approved reasons. Supervisors and administrators may need more global access to BWC recordings for QA/QI, legal review, or internal administrative reasons. Remind all users that access to BWC recordings will leave a digital footprint, and inappropriate access will carry consequences.

- **BWC Device Security.**
  - *Physical Security*. BWC devices and removable storage and collection media (*e.g.,* SD cards) should always remain physically with an employee (while engaged in operations) and then stored in a secure location.
  - *Remote Wiping/Disabling.* BWC devices should have remote wiping and disabling capability in the event of loss or theft. Remote wiping allows you to delete all data from a device without being in physical possession of the device. In contrast, remote disabling allows you to render a device unusable, but the data will remain on the device.
  - *Tracking.* BWC devices should be physically tagged (*e.g.,* RFID tagged) and tracked (*e.g.,* electronically with GPS, signed out, etc.).

- **Breaches of BWC Recordings and Devices**. Any event that qualifies as a "breach" of BWC recordings is the responsibility of your EMS agency to report. [8] Everyone at your agency should be trained to immediately report any:

  - Loss or theft of BWC devices or storage media;
  - Unauthorized internal or external access to BWC recordings; and
  - Unauthorized disclosure of a BWC recording.

[6] Be sure to consult state law regarding the deletion or destruction of BWC recordings under state public records laws.
[7] HHS recommends destroying the information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization.
[8] "Breach" has a very specific definition under HIPAA (*See,* 45 CFR § 164.402). Your agency should consult with legal counsel to determine whether an event is a breach that must be reported.

State Invasion of Privacy Laws

Most states have "invasion of privacy laws" that grant an individual the right to sue another person for intrusion into the individual's personal affairs. "Intrusion upon seclusion" (or some other similarly named right of action) is a tort[9] that many jurisdictions recognize to grant individuals that right. Consult with an attorney in your jurisdiction to determine what implications, if any, invasion of privacy laws in your state might have for BWC use by your agency.

IMPORTANT NOTE: States, and local jurisdictions vary on: (1) whether they recognize intrusion upon seclusion; and (2) the elements necessary to prove a claim.

Location Matters

Public Locations: Typically, there is little or no reasonable expectation of privacy in public places - such as a public roadway, parking lot, sidewalk, in a store, or the lobby or hallway of a facility. Invasion of privacy is much less of a concern when recording in these locations.

Private Locations: Patients have a greater expectation of privacy in private places - such as the patient's home, a private room at a facility (where the patient sleeps), or in restrooms. Invasion of privacy might be a concern in your jurisdiction when recording someone in one of these locations.

Tips for Dealing with Invasion of Privacy Issues:

In addition to following your attorney's recommendations, here are some best practices to consider:

- **Put the Patient on Notice**. When appropriate, EMS practitioners may verbally inform the patient and others at the scene that they are recording. You may also place tags on the BWC device, and post signs in ambulances stating, "Body Camera in Use" or "Recording."

- **Allow Discretion to Terminate Recording in Sensitive Situations.** You may wish to permit practitioners the discretion to turn off the BWC in sensitive situations. For example, such discretion may be warranted in incidents where the patient is: naked or partially unclothed, in the bathroom, extremely embarrassed, the victim of a sexual assault, etc. While many police departments no longer have discretion to turn off a BWC (to avoid accusations of abuse while not recording and because police are not covered by HIPAA), EMS agencies usually have the authority to turn off a BWC. Determine whether you will permit your practitioners to utilize discretion to determine when it is appropriate to not record. You must clearly define when this discretion is permitted in a policy and train your practitioners about your policy.

[9] A tort is a civil wrong (other than breach of contract) that causes an individual to suffer loss or harm, resulting in legal liability for the person who commits the wrongful act. Torts arise from the breach of a duty owed under the law.

- **Train to Deal with Requests to Stop Recording.** Your agency must provide clear guidance to practitioners about how to handle requests from the patient, the patient's authorized representative, or another individual at the scene or at a facility (sometimes hospitals will request that the practitioners not record) who asks not to be recorded. Many agencies will honor requests from patients or the patient's legal guardian not to record in many situations. But there may be incidents, such as when the patient is being combative, where you may not want to honor the request to stop recording because the BWC video may serve to protect the agency and become useful evidence of the encounter.

State Wiretap/Eavesdropping Laws

States have varying laws that may require a person recording a conversation to provide notice and obtain consent before recording. These laws are often referred to as "wiretapping" or "eavesdropping" laws because they were passed decades ago before video recording was even possible for most individuals. Most wiretap laws specifically apply to audio recording a *conversation*, not necessarily videos images of the individual. Since BWCs capture conversations, these laws must be considered. Consult with an attorney in all jurisdictions where you will use BWCs to determine what implications, if any, your state's "wiretap," or "eavesdropping" law(s) have for the use of BWCs by your agency.

The primary issue with wiretapping laws is whether the state in which you are using the BWC requires consent from the person(s) being recorded. A few states require the consent of **all parties** being recorded, while most other states require the consent of only one party. The law of the jurisdiction where the BWC is being used will apply. If you operate in different states, you need to consider the laws of every state in which you will use BWCs.

One-Party Consent States

If your state is a "one-party" consent state, which most states are, your practitioners can generally use a BWC without obtaining the consent of individuals on the scene (i.e., patients and bystanders). This is because you only need the consent of one party to the conversation. That one party consent test could be met simply because your EMS practitioner is the one who is using the BWC and interacting with the patient. In one-party states, you may still wish to have your providers apprise the patient and others that they are recording. But you are generally not required to obtain consent of other individuals in one-party consent states.

All-Party/Two-Party Consent States

A handful of states (about a dozen) require the consent of ***everybody*** involved in the conversation before the conversation can be recorded. These laws are sometimes called "two-party" consent laws but, technically, they require that all parties to a conversation give consent to the recording.

"Consent" is defined by your state law and sometimes through case law (meaning, you need an attorney to tell you what securing consent requires in your jurisdiction). In some states, the consent requirement is satisfied if all the parties are clearly notified that the interaction is being recorded, and they engage in the conversation. Their consent is implied. For example, in all-party consent states, a practitioner may make a statement such as: "We are recording." If the patient and others hear the statement and proceed to speak to the practitioners after hearing the statement, then their consent might be implied in your state if your state law permits implied consent.
For agencies in all-party consent states, consult an attorney in your jurisdiction to determine:

1. Whether your state law has an exception for EMS;
2. How EMS practitioners must obtain consent;
3. How consent should be documented or recorded; and
4. What to do if the patient or some other individual on the scene does not consent, or later revokes their consent.

IMPORTANT NOTE: Nearly all states also have exceptions to their consent requirements. Common exceptions include recordings captured by police (including BWCs), court orders, etc. Find out whether your state lists EMS as an exception to the consent requirement.

Data Retention Requirements

Determine whether any state data retention laws apply to your BWC records. If there are no state retention laws that apply to BWC recordings in your jurisdiction, then you are generally free to define the length of time for which you will retain the recordings, with some exceptions. If there are legal retention requirements, ask your local attorney to guide you through what is required.

Medical Record Retention Laws

Most states have retention requirements for medical records. There may even be specific retention requirements for EMS records in your state. The critical determination is whether BWC recordings fall within the definition of medical records under the applicable law. Your attorney will need to examine the definition and any exceptions contained in the law.

State Law Example – Arizona "Medical Records" (A.R.S. § 12-2291)

> 6. "Medical records" means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers. Medical records do not include materials that are prepared in connection with utilization review, peer review or quality assurance activities, including records that a health care provider prepares pursuant to section 36-441, 36-445, 36-2402 or 36-2917. Medical records do not include recorded telephone and radio calls to and from a publicly operated emergency dispatch office relating to requests for emergency services or reports of suspected criminal activity, but include communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the diagnosis or treatment of a person.

Arizona law states that *medical records* specifically include: "communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the **diagnosis** or **treatment**."[10] If your agency is based in Arizona, and you are recordings for "diagnosis or treatment," then your BWC recordings might be covered by this law. However, if you are using the cameras strictly for QA/QI and internal retroactive review, which most EMS agencies are, then it is possible this law would not apply to the recordings because you are not recording for diagnosis or treatment.

IMPORTANT NOTE: Carefully review your state law with your attorney and consider the purpose for which you are using the BWC recordings. If you limit the use of BWC recordings to a purpose that falls outside of a medical record retention law, you may be able to avoid having to retain the record for the period of time in the medical record retention law.

Other State Laws

States may also have data retention laws that apply to BWC recordings apart from medical record retention laws. EMS agencies must comply with all applicable data retention laws and maintain BWC recordings for the (longest) length of time required by state law. Agencies must also secure BWC videos in accordance with any applicable requirements. For example, Nevada State law requires any "data collector" that maintains "personal information," to use encryption or some other approved method to safeguard that information.[11]

Additional Considerations for Data Retention

- **HIPAA.** Address all HIPAA requirements discussed in this Guide and those recommended by your agency's legal counsel.

- **Cost.** Storing and maintaining BWC videos can be expensive because of the size of the files. There are also associated costs with maintaining a good archival system. Some costs will also be incurred managing and responding to requests for BWC records.

- **Retention in "Special Situations**." You should also retain BWC recordings in "special situations" for the length deemed necessary, which may exceed the time under your retention policy or required under state law. For example, consider retaining videos when:
  - An incident and/or record is subject to litigation.
  - An incident is flagged by your agency as a "high risk" event.
  - A video offers a good training example.
  - The BWC recording is subject to a public or another official agency request.
  - If the incident involves a patient complaint.
  - When the recording could serve as evidence of a crime.

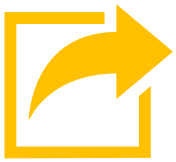
[10] A.R.S § 12-2291 (emphasis added).
[11] Nev. Rev. Stat. Ann. § 603A.215.

- **Shorter Length of Retention.** Because of the risk of breaches and high costs associated with video data retention, you should limit retention to a shorter period of time – such as 90 days when you are not subject to legal retention requirement and a special situation does not apply. Check with your attorney about the appropriate length of time and outline retention periods in a policy.

- **Outline the Purpose of BWC Recordings.** If you are using BWC videos for QA/QI purposes, outline that in a policy so it is clear that you are not treating records as part of the patient medical record. It is possible that those records may have protection under a peer review protection law in your state if you use them for the purpose of quality improvement.

State Open Records Laws

All 50 states have some form of open records law (ORL). These laws are sometimes referred to as "sunshine laws" or "right to know," or "freedom of information act" laws. Typically state open record laws require **public agencies** to make certain records available for public inspection or to provide records to the public upon request. Examples of public agencies include county, city, state, and other municipal-based fire and EMS agencies.



You must determine whether your agency is covered by your state's ORL and, if so, whether or not BWC recordings are covered by that law. If you are covered by an ORL and BWC recording are subject to disclosure under the ORL, you will need to fulfill ORL requests in accordance with the law's requirements. If you are not an agency that is covered under an ORL, then you do not have to comply with ORL requirements in your state.

Medical records are often exempted from required disclosure under ORLs.[12] But some ORLs require that the public agency redact the record and provide parts of the record that do not contain medical information.

Finally, HIPAA defers to state ORLs and provides that where an ORL law mandates that an EMS agency disclose the PHI pursuant to an ORL request, the agency is permitted by HIPAA to make the disclosure of the health information. Where a state public records law only permits, and does not mandate, the disclosure of PHI pursuant to an ORL request, or where exceptions or other qualifications apply to exempt the PHI from the state law's disclosure requirement, such disclosures are not "required by law" and are not permitted under HIPAA.

Key Questions for Your Local Attorney About ORLs

- **Is our agency subject to the state's open records law?**
- **Are BWC recordings subject to the state's open record law requirements?**
- **If we are covered by the law and BWC recordings are subject to our ORL, how must we handle requests for BWC recordings?**
- **If we are required to release BWC recordings, can we, or are we required to redact the recordings in any way?**
- **Can we charge the requestor costs associated with retrieving, disclosing, and, if allowed, redacting the recording?**
- **What is the timeframe our agency has to answer a request for BWC records?**

Body-worn Camera Policy

EMS agencies must develop a clear and carefully crafted policy on the proper use of BWCs. Education is critical and staff must be educated on your policies related to BWCs. A BWC policy should be developed in consultation with your attorney and address the following topics at a minimum:

Purpose	
	What purpose(s) will the agency use BWC recordings (*e.g.,* QA/QI, internal investigations, training, peer review, etc.)
	What purpose(s) will the agency NOT use the BWC records (*e.g.,* active treatment, diagnosis, transfer of care, etc.)
Consent	
	Whether consent needs to be obtained
	How consent must be obtained
	How consent must be documented
	What to do if the patient revokes consent after the recording has started
	What to do if the patient, the patient's personal representative, or another individual does not consent to BWC recording
Data Retention/Storage	
	BWC recording retention period
	Who is the custodian for BWC records
	Which, if any, records need to be stored longer than others
	Who is allowed to review BWC records and under what circumstances
Open Records Laws	
	How requests for BWC recordings must be handled
	Who is responsible for handling request for BWC recordings
BWC Practitioner Usage	
	How and when BWCs must be worn
	How BWCs must be secured when not in use
	How and when BWC records must be uploaded and stored
	When will BWCs be turned off

For additional questions regarding BWC policies, you should contact your agency's EMS council, State EMS Office, or an attorney licensed to practice law in your state.

About the Guide's Author:

Page, Wolfberg & Wirth is the nation's preeminent EMS, ambulance, and medical transportation industry law and consulting firm, serving thousands of private, public, and nonprofit agencies nationwide for over 20 years.