journal of healthcare
PROTECTION management
Volume 36, Number 1

Handling Active Shooter Events and Other Violence

Publication of the International Association for Healthcare Security & Safety

Leading Excellence in Healthcare Security, Safety and Emergency Management

IAHSS

A legal lens on body cameras worn by hospital security officers

William S. Marcisz, JD, CPP, CHPA

Body worn cameras (BWCs) can protect your facility from fraudulent use-of-force and misconduct claims made against security personnel, but they raise worries about invasion of privacy lawsuits. BWCs can also help to de-escalate aggressive behavior and reduce physical encounters with violent patients and visitors. The author argues that the cameras' benefits often outweigh the privacy risks, and he suggests ways to reduce the risks.

(William "Bill" Marcisz, JD, CPP, CHPA, is the Executive Director of Security, Safety & Emergency Management for the Central Florida Division of AdventHealth. He is a licensed attorney in Florida and President and Chief Consultant at Strategic Security Management Consulting, Inc., based in Orlando [www.SSMCSecurity.com]. He is a member of IAHSS.)

Body worn cameras (BWCs) were introduced for, and historically have been primarily used by, law enforcement to document investigatory actions by police officers and to defend against citizen complaints of excessive use of force [1]. BWCs are now standard equipment in a preponderance of police agencies [2]. There are many reasons why a healthcare facility might likewise want to deploy these cameras on security personnel.

For one thing, hospitals that have equipped security personnel with BWCs experience risk mitigation and liability avoidance similar to that of law enforcement agencies that have issued BWCs to police officers. Unlike traditional closed-circuit televisions (CCTVs), BWCs record both audio and video. And they are mobile, enabling recording to occur not only in hospital common areas but in all areas of the facility, where they can capture the exact nature of interactions with bellig-

erent individuals. The accuracy of the recordings has evidentiary value that can also significantly reduce fraudulent claims of inappropriate employee behavior or excessive force. This reduction, in turn, saves organizations time and money related to unnecessary or unsubstantiated litigation claims, particularly when investigating "he said–she said" scenarios. The recordings can also immediately substantiate criminal charges when employees are victims of workplace violence.

A distinct value of body worn cameras in the hospital setting is the deterring effect that live recording can have on individuals who are behaving aggressively. The prevalence and severity of workplace violence [3], combined with hospitals' zero tolerance policies, has increased expectations that hospital security departments will develop strategies to proactively de-escalate situations. The presence of BWCs can de-escalate situations before they reach the point of physical confrontation. Most aggressive patients or visitors do not expect hospital security officers to be equipped with BWCs. This element of surprise becomes a de-escalation force-multiplier when aggressive individuals (visitor, patient, or staff) become aware that their actions are being recorded. The pause that occurs when an aggressor is processing how to deal with the security officer wearing a body camera gives the officer an opportunity to redirect the person's behavior. Defusing the situation avoids physical confrontations (and subsequent injuries resulting in lawsuits), which often eliminates the need for a law enforcement response. (This lack of need for police intervention can be seen as a "community benefit" in that it frees the police to address other matters.)

Despite the field-tested benefits of having security personnel deploy BWCs, the healthcare industry has not widely embraced the cameras as part of a layered security strategy to mitigate aggressive behavior (and reduce workplace violence) [4]—for understandable reasons. Fears relating to employee and patient privacy violations, and specifically to violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), constitute the most common barrier that security directors face when discussing implementation of BWCs with their administrations.

Not surprisingly, deployment of BWCs on security officers causes apprehension among hospital administrators, risk managers, privacy and compliance personnel, human resources managers, and lawyers. There is even debate among security professionals over the benefit of BWCs in a healthcare setting [4]. However, a thoughtful legal analysis indicates that privacy concerns should not automatically bar deployment of BWCs on hospital security officers. Perceived legal barriers can often be overcome by giving administrators a deeper understanding of how body worn cameras function, by selecting a camera that has the features you require to seamlessly comply with privacy demands, and most importantly, by having a well-thought-out BWC policy and procedure.

In this article, I identify and explore the most common legal issues and questions surrounding the deployment of body worn cameras on security personnel in a healthcare environment and ways to avoid invasion-of-privacy violations. I hope that this information will be useful and dispel some of the myths about BWCs breaching privacy and creating liability for your hospital.

Although this article is a comprehensive survey of legalities, keep in mind that common law and statutes can vary from state to state. Further, legal standards can vary depending on whether a hospital is privately owned or operated by governmental entity. If you are considering implementation of a BWC program at your hospital, I strongly recommend that you have your legal department perform a review of the state and federal privacy laws in your jurisdiction as part of your vetting and decision-making process for acquiring and implementing use of BWCs by security officers. The United States currently has no statutes or state or federal case law directly governing the use of BWC technology by security personnel in hospitals. Nor has any regulatory or accreditation agency weighed in on BWCs used by a hospital's private security force. Nevertheless, your legal department can draw on other resources to guide you.

OVERALL POLICY AND PROCEDURAL CONSIDERATIONS

There are many legal issues to be considered when deploy-

ing body worn cameras on hospital security personnel. These concerns can be mitigated by implementing an effective BWC policy and standard operating procedure coupled with providing training for security staff on those guidelines.

The policy should govern the use of BWCs and the recording and storage of collected video data. The policy should also cover who can have access to recorded video data and detail who may authorize the release of the data both within the organization and to outside agencies, such as law enforcement. The policy will also need to include clear guidelines for retention and destruction of recorded data, consistent with statues of limitations, administrative laws, and other relevant laws, particularly to avoid spoliation of evidence claims (as will be discussed more fully later).

Procedures should address deployment standards and training requirements for camera use, how and when to document uses of the body cameras in written reports, and how to download and label recorded data for ready search and access. A section related to instances where recorded data from a BWC may be required to be included in patient's medical record as a digital data record set is advisable.

DEVELOPING HOSPITAL POLICY

When developing a BWC policy, make sure that the policy is easy for security staff to follow. Do not create a bunch of rules and exceptions as to where, whom, and how to record. The only places where I suggest following a no-recording rule is in restrooms, changing rooms, and employee break areas. The one exception to this rule is when a legitimate security concern or dispute is occurring in these areas—for example, when two employees are having a fistfight in a department breakroom or someone is found to be engaging in illegal activity in a restroom.

The policy should be developed by a multidisciplinary team of potential stakeholders (such as the risk management, human resources, privacy and compliance departments) and reviewed by the hospital's lawyers to ensure that the policy is compliant with state and federal law. As you will see later when I delve deeper into the potential legal issues, limiting

access to the recorded data will be the most critical component for complying with privacy laws and preventing other causes of action to be filed against the hospital. It is wise to have the hospital's legal team and information technology department assist Security in reviewing BWC products to determine what combinations of products (and data storage capabilities) will best match the organization's ability to operate and manage these tools.

In general, although the act of recording people with a body camera may be perceived as offensive or even intimidating, the actual recording of someone is not the point where the privacy issues or HIPAA violations occur. Those violations occur during the act of viewing, releasing, or publishing the recorded data. Therefore, it is critical to the protection of individual privacy rights to ensure that the body camera system has the ability to create and assign user-access levels that can be designed to limit who can retrieve, view, and release recorded data.

Example: A security officer is patrolling through the emergency department (ED) and is asked to assist with a difficult patient in exam room 5. On arrival, the officer sees that the patient is his neighbor and is being treated for alcohol abuse. The officer has every right to be in the ED, and it is unfortunate that he learns about his neighbor's alcohol problem. In this instance, there is no HIPAA or privacy violation. However, if the security officer goes home and tells his wife that their neighbor was in the hospital today being treated for alcohol abuse, he has violated HIPPA rules, and the hospital is liable.

Let's assume the same set of circumstances but add that the security officer entered his neighbor's exam room with a BWC and recorded the interaction because the neighbor was disruptive and was threatening the staff. The act of recording is not a privacy or HIPAA violation because recording is no different from the officer seeing with his own two eyes his neighbor in the exam room. If the officer maintains this information in his brain and never speaks of it to anyone, no HIPAA vio-

lation occurs. If, however, the officer (or someone else) shows the video recording of the encounter to anyone without a legitimate reason for doing so, the hospital can be liable (assuming that actual harm and damages can be proven). This showing of the recording would be analogous to the officer telling his wife about the neighbor's treatment for an alcohol problem.

As this example illustrates, recording of data may be intrusive, but it is not a privacy breach until there is an unauthorized playback or review of the recorded data. Therefore, the key to avoiding liability from BWC recordings is to safeguard video data by limiting access to it. This is best accomplished by only allowing access to the recordings by specified staff for specified reasons. For example, you may want to allow data access only to security supervisors and to certain personnel at higher managerial levels. Moreover, you may want to allow security supervisors to play back recorded data only while on duty and using an authorized computer in a secured space. Finally, I would recommend that only managerial-level personnel download or release recorded data.

TYPES OF INVASION OF PRIVACY

Invasion of privacy occurs when a person or entity intrudes on the personal life of another person without just cause [5]. Under privacy laws, the *reasonable expectation of privacy* determines whether a person has the legal right to privacy. To be held liable for invading someone's privacy, a person must unreasonably and seriously compromise the interests of another person. Whether someone is guilty, therefore, is situational and subject to tests of reasonableness [5].

The four types of invasion of privacy that can lead to a civil lawsuit include *intrusion of solitude, appropriation of name or likeness, public disclosure of private facts,* and *false light* [5]. Although situations can probably occur in which appropriation of name or likeness or false light can result in a lawsuit being filed against a hospital, intrusion of solitude and public disclosure of private facts are the causes of action most likely to stem from

security officers wearing body cameras. As such, I will focus only on those last two types of privacy invasion. [6].

Intrusion of Solitude

Intrusion of solitude involves prying into someone's private affairs or solitude in a way that would be highly offensive to a reasonable person. The invasion must occur in a place where the person had a reasonable expectation of privacy, such as in their own home, a hotel room, or in a changing room or restroom. Examples of intrusion of solitude are intercepting phone calls, peeping, taking photographs without the victim's knowledge or consent, or video recording the victim in his or her home without the person's consent or knowledge [6].

Plaintiffs must satisfy the following three elements to successfully prove their case [6]:

- the intrusion was intentional;
- the intrusion invaded the plaintiff's seclusion, private affairs, or solitude; and,
- the intrusion would be highly offensive to a reasonable person in the same situation.

The defenses to intrusion on seclusion are [6]:

- privilege (the defendant had a privilege to intrude upon the plaintiff's seclusion), and
- consent (the plaintiff gave the defendant permission to carry out the act).

Intrusion of solitude seems like a difficult case to substantiate against a hospital for a security officer using a BWC. Typically, a BWC deployment process requires the camera to be in a buffering mode until a specific incident arises that requires or permits security staff to turn on the recording function of the camera. While the camera is buffering, it is capturing and then recording over video captured generally in a 30-second incremental cycle, such that when a security officer activates the record button on the BWC, the camera will have saved the previous 30 seconds of video data and all events recorded thereafter, up to when the officer turns off the recording feature on the BWC.

If the BWC policy is adhered to, there are few situations where a hospital security officer acting in the normal course of duties would be said to invade a patient's, visitor's, or employee's

privacy. The only fathomable situation in a hospital setting where liability would attach to an intrusion of solitude claim would be when a security officer had no business being in a certain area and intentionally recorded a person while the individual was using the bathroom or was changing clothing in a locker room or dressing room.

Public Disclosure of Private Facts

Public disclosure of private facts refers to the dissemination of personal information that is not of public concern or interest, that is not part of public proceedings or records, and that would offend any reasonable person if it were published or widely disseminated [7]. When someone with access to recordings releases and publishes video data from a body worn camera, both intrusion of solitude and public disclosure of private facts require the element of intentionality for culpability. A BWC policy that limits access to who can review and release recorded data should be sufficient to prevent invasion of privacy claims from being substantiated or initiated against a hospital.

EXPECTATION OF PRIVACY IN HOSPITALS

Generally, there are four types of people in hospitals at any given time, and each group has its own expectation of privacy. Those groups are patients, visitors, employees, and trespassers. I will address the levels of privacy each group can expect, but first I should note that changes in the public's expectation of privacy in recent years can affect the success of invasion-of-privacy claims.

A determination of whether a reasonable expectation of privacy exists inside a hospital is situational and fact-specific, with an assessment focusing on who is being recorded and where in the hospital they are located. Regardless, use of BWCs almost anywhere in a hospital can usually be justified. In today's technology-driven society, CCTV use has become standard in most hospitals. Cell phones, which can record audio and video, are ubiquitous. At the same time, use of social media and of surveillance cameras has proliferated. In hospitals, few spots are truly private; there are people all around who can overhear conversations in

public areas. This wide acceptance of technology means that people should have lower expectations of privacy. As an unintended result, proving invasion of privacy claims is all the more difficult with the prevalence and proliferation of mobile technological devices.

Nevertheless, hospitals need to take precautions. If your policy restricts access for the retrieval and release of video data, you can successfully limit the chances that incidental recordings of private matters will be released and result in a breach of privacy claim. Basically, there can be no breach or damages unless the video is shown or released without proper authorization.

Patient Privacy

Arguably, patients have more privacy protections than anyone else in a hospital, but as I have noted, the expectation of privacy is situational, fluid, and subject to change depending on the totality of circumstances at any given moment.

> **Example:** A doctor may be able to go over a discharge plan with a patient in a waiting area if nobody is around to hear the discussion. However, the same discussion in the same waiting room may be inappropriate or a HIPAA violation if other people are present and within listening distance.

Under HIPPA, many kinds of information about patients (such as diagnoses, test results, care plans, and discharge instructions) are considered *protected health information* (PHI), and state statutes also cover patient rights. Security officers are rarely present when patients are conversing with a doctor or clinician about their medical condition or treatment. Typically, officers enter a patient's room only to address a behavioral concern (such as verbal disruption, aggression, or the need for restraints) or to conduct an investigation. Generally, PHI is not being discussed during incidents. Even in situations where PHI is discussed and captured by a security officer wearing a BWC, there is little risk of liability exposure if the organization has adopted a policy to safeguard data recorded by a BWC from being viewed or released.

A suggested procedure to mitigate liability risk is to enforce a policy that limits BWC activations to specific types of in-

cidents or services provided (such as investigations, patient and visitor contact, misconduct, and criminal activity). In addition, before releasing video containing PHI to outside agencies such as law enforcement, organizations should require a search warrant, investigative subpoena, court order, or administrative authorization by the hospitals risk managers or lawyers.

Employee Privacy

As is true of patients' rights, employees' rights to privacy in a hospital are situational. The rights are based on several factors, such as where a worker is located and the types of tasks the employee is expected to perform. There are also statutory and common law provisions relating to privacy considerations for employees. For the purposes of this article, the definition of *employee* can encompass physicians, contractors, and possibly vendors who regularly conduct business on a hospital site. Although most people have an expansive view of their own right to privacy, the fact is that workplace privacy is very limited in scope.

There are no laws that specifically address employee privacy as it relates to body cameras worn by an employer's security staff. However, some states prohibit surveillance of employees in certain work areas and in break rooms, locker rooms, bathrooms, or places where there may be a reasonable expectation of privacy. In general, a security officer should not turn on a BWC and record co-workers unless the officer is managing an incident in the area. If an incidental recording of a co-worker takes place, it would not be considered a breach of employee privacy if the security officer had a legitimate reason to have the BWC activated. If recorded video must be replayed or released, the hospital can either gain consent from the employee or omit the employee's image from the recorded video.

Again, when creating a BWC policy, you need to do careful research into what laws are in effect in the jurisdiction where BWCs will be used. In addition, hospitals deploying BWCs should insulate themselves from potential liability by including language in employment policies indicating that employees consent to reasonable and incidental recording (audio and video) by these

devices. Employees can also be required to sign a consent form indicating they will be subject to audio and video (BWCs, CCTV, dictation, and so on) recording as a condition of employment. Notwithstanding, a solid policy governing viewing and release of data recorded by a BWC should be sufficient to avoid liability incurred by the hospital.

Visitor Privacy

Visitors and guests are "business invitees" within a hospital and have very little legal protection in terms of privacy expectations. If you think about it, visitors and guests should have access only to areas in a hospital deemed public. If visitors venture into areas they have no business being in, then it can be argued that they occupy the status of a trespasser (see the next section) and would not have any reasonable expectation to privacy.

Except for restrooms or in limited situations where a patient's room or an examination area can be deemed to have a reasonable expectation of privacy, there are almost no other areas in a hospital which a BWC could pose a liability in terms of invasion of privacy to a visitor or guest. If security personnel are not recording visitors in a restroom, or recording private conversations taking place in a patient room, it is hard to envision a scenario in which the threshold requirements for a breach of privacy claim can be reached.

Trespassers

Trespassers are people who have no reason to be at the hospital. As such, they should have no privacy expectations when confronted by a security officer wearing a body camera who is investigating their presence. It is hard to fathom how a hospital can be found liable for recording someone who is in an area where they have no legal right to be and engaged in conduct with no permissible connection to the hospital.

In sum, few areas in hospitals are considered private when it comes to security officers wearing body cameras. To prevent liability posed by purposeful, incidental, or accidental recording of matters deemed private, the hospital's BWC policy should include specific guidelines on who can access and show recorded data and when they can do it. Release of recorded data

should be done only after consultation with, and consent from, the hospital's risk management or legal department. If the hospital has a solid BWC policy limiting the access and release of BWC data recorded by a security officer, and that policy is followed, exposure to liability for breach of privacy is very limited.

AUDIO-RELATED ISSUES: NOTICE AND CONSENT

The primary advantages of BWCs over CCTV are the BWC's mobility for reaching areas where CCTV coverage is not available and the ability to acquire audio documentation of what is being said during investigations and encounters. However, audio recording by BWCs may in some cases be subject to state and federal wiretapping laws. Therefore, it follows that the concepts of providing "notice" of recording conversations and "consent to be recorded" can pertain to the audio aspect of anything recorded by BWCs. Because of this, when developing a BWC policy, a necessary first step is to determine whether your hospital is located in a "one-party" or "two-party" state; that determination will affect requirements for who and how many people must give consent to an audio recording.

Most states are one-party-consent states, meaning that only one party has to give consent to be recorded. For example, Bob calls Lisa on the phone. Bob wants to record the conversation. By recording the conversation, Bob's consent is implied because he is aware the conversation is being recorded. It is irrelevant that Lisa is not aware of the recording and has not also given her consent.

If your hospital is located in one of the 11 states that require "two-party consent," you will need to provide notice of the recording and attain everyone's consent [8]. (For this reason, "two-party" consent may also be known as "all-party" consent). The eleven "two-party consent" states are California, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. The laws requiring notice are sometimes referred to as "two-party consent" laws.

If your hospital is located in a two-party consent state, you will want to notify everyone entering the hospital facility that

they are subject to being recorded by audio and video. Notice can be given by simply placing signs at all public entrances advising patients and guests they may be subject to audio and video recording. I recommend that the word "audio" be included and emphasized on the sign. (A simple image of a camera without the word "audio" or without any indication that audio recording is possible would probably not be deemed sufficient notice of audio recording.) Any patient or guest who passes the sign and enters the facility can be said to have been placed on notice of potential recording, and by entering the hospital facility they tacitly accept these terms. This posting should cover the notice provision for most patients and visitors who enter the building.

In addition to placing the signs at entrances, hospitals should also obtain recording consent from employees, by having them sign general disclosures when they accept terms of employment on hiring. Almost without exception, consent to be recorded by a security officer's body camera falls into these general employment terms. As such, it is recommended that a review of all pre-employment paperwork, forms, manuals, and contracts be conducted to ensure that consent to BWC recording can be reasonably said to fall within the terms of employment. If your organization's pre-employment disclosures do not cover recording by BWCs, I recommend executing a separate consent for all employees and amending the pre-employment documents to include consent provisions for recording in audio and video formats.

The policy governing use of BWC and training should include a standardized mandatory script that security officers should use each time they activate the camera. On activating the camera, the officer could simply state, "Good afternoon. I am here to assist. I just want you to be aware I have activated my body camera and our discussions are being audio and video recorded." This scripting is strategically designed both as a common courtesy and as an added way to provide notice in case someone did not see the sign at the entrance. This scripting also gives people who are being recorded an opportunity to decline consent, and it ensures

that the hospital has provided the requisite notice to comply with a two-party consent statute.

It is rare for someone to decline consent to recording, but I should note that refusal of consent to be recorded extends only to the audio portion of BWC recording. If someone refuses consent, the officer can simply mute or turn off the audio recording feature on the BWC and continue to video record the interaction. Although you will not capture what is being said in the audio, important video evidence of the interaction showing demeanor and body language can prove to be just as valuable from a forensic standpoint. It also bears mentioning that if people are recording the incident with cell phones or other devices (and particularly if the person who refuses to give consent is doing such recording), security officers should continue recording both audio and video on their body cameras.

VIDEO VOYEURISM

One reason to restrict access to video playback is to protect the hospital from having its body camera system used to record or transmit images of people in patient rooms or other areas where privacy is expected. Criminal statutes on video voyeurism prohibit a person, for his or her own amusement, entertainment, sexual arousal, gratification, or profit, from using, installing, or allowing another person to use or install an imaging device to secretly view, broadcast, or record a person who is exposing the body at a time when that person has a reasonable expectation of privacy (*see* Florida Statute 810.145). Although this activity is clearly criminal, it does place the hospital at potential risk for various legal actions relating to negligent hiring, supervision, and retention or to infliction of emotional distress.

This possibility does not mean that if a security officer happens to record a patient who is undressed, the act of recording constitutes a crime or will cause the hospital to be liable for damages—particularly when that patient (or a visitor) is being disruptive or aggressive. Once a security officer begins recording a patient who is undressed, it is generally recommended that the officer continue recording through to the end of the incident. Remember, if access to

video playback is limited to only a few supervisory or managerial staff members, there is little risk that the recordings will be used for voyeurism. Although turning off a body camera when someone is undressed may seem like the decent thing to do, continuing to record the entire incident is recommended to protect the security staff and the hospital from claims of improper conduct later on. In fact, turning the camera off may create an inference that the officer(s) involved did something wrong and wanted to cover it up.

RETENTION OF RECORDINGS AND SPOLIATION OF EVIDENCE

When acquiring a body camera system, factor in the need to store recorded data in a way that complies with the retention requirements of statues of limitations and statues of repose in your state. In most cases, storing data for 10 years should be enough; however, you should research the length of time your state may require you to preserve evidence. Some BWC systems have unlimited storage, which is an ideal solution because it allows you to save all data recorded for an indefinite amount of time.

If this is cost prohibitive, you could consider saving only data relating to recorded incidents that may incur civil liability. An unfortunate caveat in doing so is that you may place an unreasonable burden on security staff, who as lay persons will need to determine which incidents may result in litigation. In addition, your organization may risk a spoliation of evidence claim. (*Spoliation of evidence* is the failure to preserve evidence that could reasonably be anticipated to be relevant to a possible case.) Courts frown on spoliation of evidence. It would be a better practice to spend the extra money on data storage than risk a spoliation of evidence claim, particularly in situations where there is a mistaken or fraudulent claim of malfeasance alleged against your hospital. To rule that spoliation occurred, courts will generally require that the evidence existed at one time; that the Party had a duty to preserve the evidence; and that the evidence was critical to the opposing Party's ability to prove its prima facie case or defense [9].

A BWC policy should include

mandatory retention of certain types of incidents, such as slip and falls, anything involving injury, and all patient contact calls (regardless of whether or not security officers are called on to take action and even when the patient is docile or compliant). This rule is important because sometimes false claims are later initiated against the hospital even for routine encounters where nothing out of the ordinary occurred. If there is no BWC recording available, a plaintiff might make and ultimately prevail on a spoliation claim for damages, even if the underlying cause is baseless or fraudulent.

Because each state has its own separate laws relating to statutes of limitation and spoliation of evidence, it is best to get an opinion from your hospital's legal experts on issues relating to retention of recorded data.

CONSTITUTIONAL PRIVACY RIGHTS

Your BWC policy and procedures will also need to take into account statutes and common law opinions on constitutional rights to privacy—both as protected by the U.S. Constitution and by the constitution of the state or states in which your facility resides. Constitutional law rulings can affect your hospital if it is owned or operated by a governmental entity or taxing district or when a privately owned hospital employs or contracts with governmental employees. The latter may include employing Public Act Security Police Officers, hiring or posting active duty or off-duty police officers in your hospital, or providing a local police agency with a substation in your hospital.

There is an entire body of federal constitutional law, and each state may have its own set of constitutional laws dedicated to privacy. This is another reason why your organization should perform legal research and ensure that your BWC policy complies with state and federal constitutional privacy rights.

PATIENT'S RIGHTS STATUTES

States generally have statutes relating to the patients' rights, such as the right to privacy and the right to dignity. I do not know of any state that has express provisions governing the video or audio recording of patients in hospitals. Someday, however,

the proliferation of cell phones and other recording devices will probably spur a legislature to evaluate their impact on patients' rights statutes. Hence, you will want to include patients' rights statues in any legal analysis conducted to guide the development of BWC policies and procedures.

PATIENT DATA RECORDS

Some observers have suggested that body worn cameras could eventually be considered for use outside of security, in the clinical realm, where BWCs might be worn by physicians, nurses, ED employees, paramedics, and emergency medical technicians. After all, the cameras could help to ensure accountability and document the care that was provided. If the cameras are used in that way, consideration should be given to whether clinical BWC recordings should be added to the patient's medical records as a digital data record set.

Video surveillance could be found to constitute protected health information under HIPPA (*see:* 45 C.F.R. § 160.103). If a BWC identifies a patient receiving care in a hospital, the recorded data can potentially be deemed protected health information. This is because PHI is considered to be any information about health status or a provision of or payment for health care that is created or collected by a "covered entity" and can be linked to the specific individual. As such, any policies and procedures relating to BWCs in your healthcare facility need to address the confidentiality and potential disclosure of recorded data to ensure compliance with 45 C.F.R. Section 164.524, which governs the access for individuals to their PHI.

I have already said that, for the most part, data recorded by security officers using BWC falls outside of protected health information as contemplated by HIPAA. This is because security officers are seldom present when health information is being discussed, where actual care is being provided, or when billing information is being disseminated. Therefore, nearly all BWC data acquired on patient contact calls typically fall outside the definition of PHI. However, for those rare instances where digitally recorded data from a BWC can be considered PHI, the BWC policy should contain a section re-

lating to digital data sets stating, "at the discretion and direction of physicians or nursing staff, Security will preserve, and label video related to a patient's care and transmit this data set to the Health Information Department for inclusion in the patient's electronic medical chart."

CONCLUSION

Without question, body cameras worn by security officers are a very effective tool to deter violence and assist in de-escalation of aggressive people. BWCs greatly assist investigations relating to employee conduct and to complaints about excessive use of force by security officers. When properly deployed, they will prove to be an excellent component of a strategy for risk mitigation and liability avoidance. BWCs add a layer of accountability for security staff and, over time, can elevate the level of professionalism by the team. As an unintended ancillary benefit, BWCs have also proven to positively change the behaviors of physicians and other clinicians who might otherwise antagonize or act as aggressors in certain situations. In a sense, by adding a layer of accountability, BWCs can be said to have a positive influence on organizational culture.

The legal issues surrounding the implementation of body cameras worn by security officers do warrant a legal analysis prior to deployment. There are many issues and answers that need to be addressed on a state-by-state basis. Also, as a caveat, it should be noted that there may be other issues or legal implications not mentioned in this article. However, a solid policy guiding BWC use and the storage of, and access to, digitally recorded data can make this technology easy to use in the field and ensure that use of BWCs will not incur liability.

References

1. Miller, L., Toliver, J., & Police Executive Research Forum. (2014). *Implementing a body-worn camera program: Recommendations and lessons learned.* Washington, DC: Office of Community Oriented Policing Services.

2. Body cameras now standard gear for Florida cops. But not in Tampa Bay. (2018, March 19). *Tampa Bay Times.* https://www.tampabay.com/news/publicsafety/Body-cameras-now-standard-gear-for-Florida-cops-But-not-in-Tampa-Bay_166350517

3. The Joint Commission Sentinel Event Alert, Issue 45 (2010, June 3; Revised February 2019). *The Joint Commission.* https://www.jointcommission.org/sentinel_event_

alert_issue_45_preventing_violence_in_the_health_care_setting_/

4. Body cameras: A legal tool or legal liability? *Hospital Safety Center*. http://www.hospitalsafetycenter.com/content/322323/topic/WS_HSC_HSA.html

5. Invasion of privacy law and legal definition. *USLegal*. https://definitions.uslegal.com/i/invasion-of-privacy/

6. Intrusion of solitude lawyers. *LegalMatch*. https://www.legalmatch.com/law-library/article/intrusion-of-solitude-lawyers.html

7. Content team. Invasion of Privacy. *Legal Dictionary*. https://legaldictionary.net/invasion-of-privacy/

8. Laws on recording conversations in all 50 states. (Updated 2019, June 18). *Matthiesen, Wickert & Lehrer*. https://www.mwl-law.com/wp-content/uploads/2018/02/RECORDING-CONVERSATIONS-CHART.pdf

9. McNamara, M.A. (2017, March 16). Spoiler alert—duty to preserve evidence. *South Florida Trial Practice*. https://southfloridatrial.foxrothschild.com/general-litigation/spolier-alert-duty-to-preserve-evidence/